53-1001355-01
28 July 2009

Data Center Fabric Manager Professional

User Manual

Supporting DCFM 10.3.X

BROCADE

Copyright © 2007-2009 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, IronPoint, IronShield, IronView, IronWare, JetCore, NetIron, SecureIron, ServerIron, StorageX, and TurboIron are registered trademarks, and DCFM, Extraordinary Networks, and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

The following table lists all versions of the DCFM Professional User Manual.

Document Title	Publication Number	Summary of Changes	Publication Date
DCFM Professional User Manual	53-1001079-01	First release	August 2008
DCFM Professional User Manual	53-1001195-01	Second release.	December 2008
DCFM Professional User Manual	53-1001259-01	Revised for 10.2.X release.	April 2009
DCFM Professional User Manual	53-1001355-01	Revised for 10.3.X release.	July 2009

Contents

About This Document

In this chapter xix
How this document is organized xix
Supported hardware and software xx
What's new in this document xxii
Document conventions xxiii
Text formatting xxiii
Notes, cautions, and warnings xxiv
Key terms xxiv
Notice to the reader xxiv
Additional information xxv
Brocade resources xxv
Other industry resources xxv
Getting technical help xxvi
Document feedback xxvii

Chapter 1 User interface overview

In this chapter 1
User interface components 1
Menu bar 3
Toolbar 10
View All tab 11
Port Display buttons 11
Product List 11
Connectivity Map 12
Toolbox 13
Master Log 13
Minimap 14
Status bar 15
Icon legend 16
Product icons 16
Group icons 17
Port icons 17
Product status icons 18
Event icons 18
Shortcut menus 19

Feature-to-firmware requirements 31

Accessibility features for the Management application 33
Keyboard shortcuts 33
Look and Feel 34

Chapter 2 Discovery

In this chapter 37

Fabric discovery overview 37
FCS policy and seed switches 38
Discovering fabrics 39
Configuring SNMP credentials 42
Reverting to a default SNMP community string 43
Deleting a fabric 43

Host discovery 44
Discovering Hosts by IP address or hostname 44
Importing Hosts from a CSV file 45
Importing Hosts from a Fabric 46
Configuring Brocade HBA credentials 47
Configuring virtual machine credentials 48
Editing Host credentials 49
Removing a Host from Discovery 50

Viewing the discovery state 50

Troubleshooting discovery 51

Fabric monitoring 51
Monitoring discovered fabrics 52
Stop monitoring of a discovered fabric 52

Seed switch 53
Seed switch requirements 54
Seed switch failover 54
Changing the seed switch 54

Chapter 3 Application Configuration

In this chapter 57

Management server and client 58
Logging into a server 60
Logging into a remote client 61
Changing your password 62
Changing the database user password 63
Viewing active sessions 63
Disconnecting users 64
Viewing server properties 64
Customizing the main window 65
Customizing the application 66
Searching for a device in the connectivity map 70

Data backup 70
What is backed up? 70
Management server backup 70
Configuring backup to a writable CD 71
Configuring backup to a hard drive 72
Configuring backup to a network drive 73
Enabling backup 75
Disabling backup 75
Viewing the backup status 75
Changing the backup interval 76
Starting immediate backup 76
Reviewing backup events 77

Data restore 77
Restoring data 78
Restoring data to a new server 78

Display 79
Resetting your display 79

End node display 80
Displaying end nodes 80

Ethernet events 81
Enabling Ethernet events 81
Disabling Ethernet events 82

Event storage 82
Configuring event storage 82

Flyovers 83
Configuring flyovers 83
Turning flyovers on or off 86
Viewing flyovers 86

Names 87
Setting names to be unique 87
Setting names to be non-unique 88
Fixing duplicate names 88
Viewing names 89
Adding a name to an existing device 89
Adding a name to a new device 90
Removing a name from a device 90
Editing names 90
Exporting names 91
Importing Names 91
Searching by name 92
Searching by WWN 92

Security 93
Configuring the server name 93
Setting the CHAP secret 94
Configuring login security 94
Configuring the login banner display 95
Disabling the login banner 95

Software Configuration 96
Client export port 96
Discovery 97
FTP/SCP overview 98
IP Configuration 102
Memory allocation 106
Server port 108
Support mode 109

Fabric tracking 110
Enabling fabric tracking 110
Disabling fabric tracking 110
Accepting changes for a fabric 111
Accepting changes for a device 111

Third-party tools 111
Starting third-party tools from the application 111
Launching a Telnet session 112
Launching an Element Manager 112
Launching Web Tools 113
Launching FCR configuration 113
Launching HCM Agent 114

Topology layout 115
Customizing the layout of devices on the topology 116
Customizing the layout of connections on the topology 116
Changing a group's background color 117
Reverting to the default background color 118
Changing the product label 118
Changing the port label 118
Changing the port display 119
Grouping on the topology 119

Chapter 4 Server Management Console

In this chapter 123

Server management console overview 123
Launching the SMC on Windows 123
Launching the SMC on Linux and Solaris 124

Services 124
Monitoring and managing Management application services 124
Refreshing the server status 125
Stopping all services 125
Starting all services 125
Restarting all services 126

Changing server port numbers 126

Restoring the database 127

Capturing technical support information 128

Upgrading HCM on the Management server 129

Chapter 5 Device Configuration

In this chapter 131

Configuration repository management 131
Saving switch configurations 132

Device properties 133
Viewing properties 133
Adding a property label 136
Editing a property label 136
Deleting a property label 137
Editing a property field 137

Enhanced group management 137

Firmware management 138
Displaying the firmware repository 138
Importing a firmware file and release notes 139
Deleting a firmware file 140
Downloading firmware 141

HBA server mapping 142
Creating a new HBA server 143
Renaming an HBA server 143
Deleting an HBA server 144
Viewing Server properties 144
Associating an HBA with an HBA server 144
Importing HBA-to-server mapping 145
Removing an HBA from a HBA server 146

Ports 147
Viewing port connectivity 147
Refreshing the port connectivity view 150
Enabling a port 150
Disabling a port 150
Filtering port connectivity 151
Viewing port details 152
Viewing ports and port properties 153
Port types 156
Showing connected ports 156
Viewing port connection properties 157
Determining inactive iSCSI devices 159
Determining port status 159
Viewing port optics 159

Port Auto Disable 161
Viewing the port auto disable status 161
Enabling port auto disable on individual ports 162
Enabling port auto disable on all ports on a device 162
Disabling port auto disable on individual ports 163
Disabling port auto disable on all ports on a device 163
Unblocking ports 163

Device Technical Support 164
Scheduling technical support information collection 164
Starting immediate technical support information collection 165
Viewing technical support information 165
E-mailing technical support information 166
Deleting technical support files from the repository 166

Failure data capture 167
Enabling failure data capture 167
Disabling failure data capture 168
Purging failure data capture files 168
Configuring the failure data capture FTP server 168
Viewing the upload failure data capture repository 169

Chapter 6 Fault Management

In this chapter 171

Fault management overview 171

Event logs 172
Viewing event logs 172
Copying part of a log entry 173
Copying an entire log entry 173
Exporting the entire log 174
E-mailing all event details from the Master Log 174
E-mailing selected event details from the Master Log 174
E-mailing a range of event details from the Master Log 175
Displaying event details from the Master Log 175
Copying part of the Master Log 176
Copying the entire Master Log 176
Exporting the Master Log 177
Filtering events in the Master Log 177

Event policies 179
Policy types 179
Policy triggers 180
Policy actions 180
Adding an event policy 180
Adding an ISL offline policy 181
Adding a PM threshold crossed policy 182
Adding a security violation policy 183
Defining the broadcast message action 184
Defining the launch script action 185
Defining the send e-mail action 186
Configuring support data capture action 187
Activating a policy 187
Deactivating a policy 187
Deleting a policy 188

Duplicating an event policy 188
Duplicating an ISL offline policy 189
Duplicating a PM threshold crossed policy 190
Duplicating a security violation policy 191
Editing an event policy 192
Editing an ISL offline policy 193
Editing a PM threshold crossed policy 194
Editing a security violation policy 195
Viewing events 195

Event notification 196
Configuring e-mail notification 196
Setting up advanced event filtering 197

SNMP trap and informs registration and forwarding 199
Registering the management server 199
Registering a different Management application server. 199
Removing a host server 200
Enabling trap forwarding 200
Adding an SNMPv1 destination 200
Adding an SNMPv3 destination 201
Editing a destination 202
Removing a destination 202
Disabling trap forwarding 202
Enabling SNMP informs 203
Disabling SNMP informs 203

Syslog forwarding 204
Registering the management server 204
Registering a host server 205
Removing a host server 205
Adding a destination 205
Editing a destination 206
Removing a destination 206
Enabling Syslog forwarding 206
Disabling Syslog forwarding 207

Chapter 7 Performance Data

In this chapter 209

Performance overview 209
Performance measures 209
Performance management requirements 210

Real-time performance data 215
Generating a real-time performance graph 216
Filtering real-time performance data 217
Exporting real-time performance data 218
Clearing port counters 218

Chapter 8 Reports

In this chapter 219
Report types 219
Generating reports 220
Viewing reports 220
Exporting reports 221
Printing reports 221
Deleting reports 222
Generating zoning reports 222

Chapter 9 Host management

In this chapter 223
About host management 223
Host discovery 224
Connectivity map 224
HBA server mapping 225
Host performance management 226
Host fault management 227
HBA events 227
Event policies 227
Filtering event notifications 227
Syslog forwarding 228
Host Connectivity Manager 228
HCM features 228
Launching HCM 229
Host security authentication 230
Configuring security authentication using the Management application 230
supportSave 232

Chapter 10 Fibre Channel over IP

In this chapter 233
FCIP services licensing 234
FCIP Concepts 234
IP network considerations 234
FCIP platforms and supported features 235
FCIP trunking overview 237
Load leveling and failover using FCIP trunking 237
Adaptive Rate Limiting and QoS priorities 238
FCIP Trunk design considerations 238
IPSec implementation over FCIP 239

Open systems tape pipelining 240
FCIP Fastwrite and Tape Acceleration 240
Virtual Port Types 241
FCIP configuration guidelines 242
Additional guidelines for tunnel advanced settings 243
Data compression 243
Open systems tape pipelining (OSTP) 243
IPSec and IKE policies 243
FICON emulation features 244
Configuring an FCIP tunnel 245
Adding an FCIP circuit 247
Configuring FCIP Circuit Advanced Settings 248
Configuring FCIP tunnel advanced settings 249
Compression, OSTP, and Tperf 249
Enabling and disabling compression 250
Enabling Open Systems Tape Pipelining (OSTP) 250
Enabling Tperf test mode 250
Configuring IPSec and IKE policies 251
Configuring FICON emulation 252
Viewing FCIP connection properties 253
Viewing General FCIP properties 254
Viewing FCIP FC port properties 255
Viewing FCIP Ethernet port properties 256
Editing FCIP tunnels 257
Editing FCIP circuits 258
Disabling FCIP tunnels 259
Enabling FCIP tunnels 259
Deleting FCIP tunnels 260
Disabling FCIP circuits 260
Enabling FCIP circuits 260
Deleting FCIP Circuits 260
Displaying FCIP performance graphs for FC ports 261
Displaying FCIP performance graphs for Ethernet ports 261
Displaying link details for FCIP tunnels 261
Displaying tunnel properties from the FCIP tunnels dialog box . . . 262
Displaying FCIP circuit properties from the FCIP tunnels dialog box 263
Displaying switch properties from the FCIP Tunnels dialog box . . . 264
Displaying fabric properties from the FCIP Tunnels dialog box . . . 265
Troubleshooting FCIP Ethernet connections 266

Chapter 11 Fibre Channel over Ethernet

In this chapter 267

FCoE overview 267
DCB exchange protocol 267

Enhanced Ethernet features 268
Enhanced transmission selection. 268
Priority-based flow control 268
Ethernet jumbo frames 268

FCoE protocols supported 269
Ethernet link layer protocols supported 269
FCoE protocols 269

CEE configuration 270
Opening the CEE Configuration dialog box. 270
CEE configuration tasks 271

Switch policies. 272
CEE map and Traffic Class map 272
LLDP profiles 272
Access control lists 272
Spanning Tree Protocol policy 273
802.1x policy 273

Link aggregation groups 273
Editing a CEE switch 275
Editing a CEE port 276
Editing a LAG 277
Enabling a CEE port or LAG 279
Disabling a CEE port or LAG 280
Deleting a LAG 280

CEE Performance 281
Real Time Performance Graph 281
Historical Performance Graph. 282

QoS configuration 282
Enhanced Transmission Selection 282
Priority-based flow control. 283
Creating a CEE map. 283
Editing a CEE map 285
Deleting a CEE map 286
Duplicating a CEE map 286
Assigning a CEE map to a port or link aggregation group. . . . 287
Creating a traffic class map 288
Editing a traffic class map. 288
Deleting a traffic class map 289
Duplicating a traffic class map 289
Assigning a traffic class map to a port or link aggregation group290

LLDP-DCBX configuration 291
Adding an LLDP profile 292
Editing an LLDP profile 293
Deleting an LLDP profile 293
Duplicating an LLDP profile 294
Assigning an LLDP profile to a port or ports in a LAG 295

Access Control List configuration 296
Adding an ACL to a switch 296
Editing the parameters of an ACL 299
Deleting an ACL 299
Duplicating an ACL profile 300
Assigning an ACL to a port or link aggregation group 301

Spanning Tree Protocol configuration 302
Enabling Spanning Tree Protocol 302
Setting Spanning Tree parameters for a switch 303
STP configurable parameters at the port or LAG level 306

802.1x authentication 307
Enabling 802.1x authentication 307
Disabling 802.1x 308
Setting 802.1x parameters for a port 308

Virtual FCoE port configuration 310
Viewing virtual FCoE ports 310
Clearing a stale entry 311

Chapter 12 Encryption configuration

In this chapter 313

Gathering information 314

Encryption user privileges 315

Encryption Center features 316

Smart card usage 316
Registering authentication cards from a card reader 317
Registering authentication cards from the database 318
De-registering an authentication card 318
Using authentication cards 318
Registering system cards from a card reader 319
De-registering a system card 319
Enabling or disabling the system card requirement 320

Viewing and editing switch encryption properties 320
Saving the public key certificate 323
Enabling the encryption engine state 323
Disabling the encryption engine state 323

Viewing and editing group properties 324
General tab. 325
Members tab 325
Consequences of removing an encryption switch 326
Security tab 328
HA Clusters tab. 329
Engine Operations tab 329
Link Keys tab 330
Tape Pools tab 331
Encryption Targets dialog box. 333
Redirection zones 335
Creating a new encryption group 336
Adding a switch to an encryption group. 344
Creating high availability (HA) clusters 347
Removing engines from an HA cluster 348
Swapping engines in an HA cluster 349
Failback option. 349
Invoking failback 349
Adding encryption targets. 350
Configuring hosts for encryption targets 357
Adding Target Disk LUNs for encryption 358
Adding Target Tape LUNs for encryption 361
Configuring encrypted storage in a multi-path environment 362
Master keys 363
Active master key 363
Alternate master key 364
Master key actions. 364
Reasons master keys can be disabled. 364
Saving the master key to a file 364
Saving a master key to a key vault 366
Saving a master key to a smart card set 367
Restoring a master key from a file 369
Restoring a master key from a key vault 370
Restoring a master key from a smart card set. 371
Creating a new master key 372
Zeroizing an encryption engine 373
Tracking Smart Cards 375
Encryption-related acronyms in log messages 376

Chapter 13 Zoning

In this chapter 377

Zoning overview. 377
- Special zones 377
- Online zoning 378
- Accessing zoning 378
- Zoning naming conventions 378

Zoning configuration 379
- Configuring zoning for the SAN 379
- Creating a new zone 380
- Viewing zone properties 381
- Adding members to a zone 381
- Creating a new member in a zone by WWN 382
- Creating a new member in a zone by domain, port index. . . . 383
- Creating a new member in a zone by alias 384
- Enabling or disabling the default zone for fabrics 385
- Enabling or disabling safe zoning mode for fabrics. 386
- Creating a new zone alias 387
- Editing a zone alias 387
- Removing an object from a zone alias 388
- Exporting zone aliases. 389
- Renaming a zone alias 389
- Creating a zone configuration 389
- Viewing zone configuration properties 390
- Adding zones to zone configurations 391
- Activating a zone configuration. 391
- Deactivating a zone configuration 393
- Refreshing a zone database 394
- Merging two zone databases 394
- Saving a zone database to a switch 396

Traffic isolation zoning 397
- Configuring traffic isolation zoning 397
- Creating a traffic isolation zone 398
- Adding members to a traffic isolation zone 399
- Enabling a traffic isolation zone 400
- Disabling a traffic isolation zone 400
- Enabling failover on a traffic isolation zone 401
- Disabling failover on a traffic isolation zone 401

Zoning administration. 402
- Comparing zone databases. 402
- Setting change limits on zoning activation. 404
- Deleting a zone 405
- Deleting a zone alias 406
- Deleting a zone configuration 406
- Clearing the fabric zone database 407
- Duplicating a zone 407
- Duplicating a zone alias 408
- Duplicating a zone configuration 408

Finding a member in one or more zones 409
Finding a zone member in the potential member list 409
Finding zones in a zone configuration 410
Finding a zone configuration member in the zones list 410
Listing zone members 411
Removing a member from a zone. 411
Removing a zone from a zone configuration 412
Renaming a zone 412
Renaming a zone configuration 413
Replacing zone members 414

Chapter 14 Troubleshooting

In this chapter 415

FC troubleshooting 415
Tracing FC routes 416
Troubleshooting device connectivity. 417

IP troubleshooting. 419
Configuring IP ping 419
Tracing IP routes. 421
Viewing FCIP tunnel performance. 422

Client browser troubleshooting 423

Fabric tracking troubleshooting 424

Professional edition login troubleshooting 424

Supportsave troubleshooting 424

Zoning troubleshooting. 425

Appendix A Supported Key Management Systems

In this appendix. 427

Key management systems 427

The NetApp Lifetime Key Manager 428
The NetApp DataFort Management Console 428
Obtaining and importing the LKM certificate. 429
Exporting the KAC certificate signing request 430
Submitting the CSR to a certificate authority 430
Importing the signed KAC certificate 431
Registering the certificates 432
LKM appliance cluster support. 434
Establishing the trusted link 434

The RSA Key Manager 436
Obtaining and Importing the RKM certificate 436
Exporting the KAC certificate signing request (CSR) 436
Submitting the CSR to a certificate authority 437
Importing the signed KAC certificate 437
Uploading the KAC and CA certificates onto the RKM appliance. 438
RKM Appliance cluster support 440

The HP Secure Key Manager 440
Obtaining a signed certificate from the HP SKM appliance software 441
Importing a signed certificate 442
Exporting the KAC certificate request 443
Setting up a Brocade user 443
Registering the Brocade user name and password on the switch 444
Setting up the local certificate authority 444
Adding the local CA to the trusted CAs list 445
Adding a server certificate for the SKM appliance 445
Downloading the local CA certificate file 446
Creating an SKM Key vault High Availability cluster 447
Copying the local CA certificate 448
Adding an HP SKM appliance to a cluster 448
Signing the KAC certificate 449
Importing a signed certificate (SAN Management program) .450

Thales Encryption Manager for Storage 451
Adding a client 451
Signing the CSR 452
Registering the certificates 453

Appendix B Sybase and Derby Database Fields

In this appendix 455

Database tables and fields 456
Capability 456
Client_view 457
Collector 460
Config 463
Connected end devices 465
Device 466
EE- Monitor 473
Event/FM 475
Fabric 481
FC Port Stats 484
FCIP 487
FCIP Tunnel Stats 490
GigE Port Stats 492
ISL 494
License 497
Meta SAN 498
Network 500
Others 501
Port Fencing 502

Quartz 503
Reports 506
Role Based Access Control 506
SNMP 509
Stats 512
Switch 514
Switch details 519
Switch port 524
Switch SNMP info 529
Threshold 531
User Interface 532
Zoning 1 533
Zoning 2 535

Index

About This Document

In this chapter

- How this document is organized xix
- Supported hardware and software. xx
- What's new in this document xxii
- Document conventions xxiii
- Additional information xxv
- Getting technical help xxvi
- Document feedback xxvii

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible. This document supports DCFM 10.3.0 and later.

The document contains the following components:

- Chapter 1, "User interface overview," provides a high-level overview of the user interface.
- Chapter 2, "Discovery," describes how to discover SANs and hosts.
- Chapter 3, "Application Configuration," provides Management application configuration instructions.
- Chapter 4, "Server Management Console," provides information on using the Server Management Console to stop and start the Management application services, back up the Management application database, and capture technical support information.
- Chapter 5, "Device Configuration," provides device configuration instructions.
- Chapter 6, "Fault Management," provides event management instructions.
- Chapter 7, "Performance Data," provides information on how to manage performance.
- Chapter 8, "Reports," provides instructions for generating reports.
- Chapter 9, "Host management," provides information on how to configure an HBA.
- Chapter 10, "Fibre Channel over IP," provides information on how to configure an FCIP.
- Chapter 11, "Fibre Channel over Ethernet,"provides information on how to configure an FCoE.
- Chapter 12, "Encryption configuration," provides information on configuring encryption.
- Chapter 13, "Zoning," provides zoning configuration instructions.
- Chapter 14, "Troubleshooting," provides troubleshooting details.

- Appendix A, "Supported Key Management Systems," provides information about supported key management systems.
- Appendix B, "Sybase and Derby Database Fields," provides reference information related to databases.

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for DCFM 10.3.X, documenting all possible configurations and scenarios is beyond the scope of this document.

The following firmware platforms are supported by this release of DCFM 10.3.X:

- Fabric OS 5.0 or later in a pure Fabric OS fabric
- Fabric OS 6.0 or later in a Mixed Fabric

  For platform specific Fabric OS requirements, refer to the Table 1 footnotes.

NOTE
Discovery of a Secure Fabric OS fabric in strict mode is not supported.

The hardware platforms in the following table are supported by this release of DCFM 10.3.X.

TABLE 1 Supported Hardware

Device Name	Terminology used in documentation
Brocade 200E switch	16-port, 4 Gbps FC Switch
Brocade 300 switch[6]	24-port, 8 Gbps FC Switch
Brocade 4012 switch	Embedded 12-port, 4 Gbps FC Switch
Brocade 4016 switch	Embedded 16-port, 4 Gbps FC Switch
Brocade 4018 switch	Embedded 18-port, 4 Gbps FC Switch
Brocade 4020 switch	Embedded 20-port, 4 Gbps FC Switch
Brocade 4024 switch[5]	Embedded 24-port, 4 Gbps FC Switch
Brocade 4100 switch	32-port, 4 Gbps FC Switch
Brocade 4900 switch[2]	64-port, 4 Gbps FC Switch
Brocade 5000 switch[3]	32-port, 4 Gbps FC Interop Switch
Brocade 5100 switch[6]	40-port, 8 Gbps FC Switch
Brocade 5300 switch[6]	80-port, 8 Gbps FC Switch
Brocade 5410 embedded switch[6]	8 Gbps 12-port Embedded Switch
Brocade M5424 embedded switch	8 Gbps 24-port Embedded Switch
Brocade 5470 embedded switch	8 Gbps 16-port Embedded Switch
Brocade 5480 embedded switch[6]	8 Gbps 24-port Embedded Switch

TABLE 1 Supported Hardware

Device Name	Terminology used in documentation
Brocade 7500 Extension switch[1]	4 Gbps Router, Extension Switch
Brocade 7500E Extension switch[1]	4 Gbps Extension Switch
FR4-18i Blade	4 Gbps Router, Extension blades
Brocade AP7600 switch[6]	4 Gbps 32-port Switch
Brocade 7800 Switch[11]	8 Gbps 16-FC ports, 6-Gbit ports Extension Switch
Brocade 8000 switch[10]	8 Gbps 16-FC-ports, 10 GbE8-Ethernet Port Switch
Brocade 415 Host Bus Adapter	4 Gbps 1-port HBA
Brocade 425 Host Bus Adapter	4 Gbps 2-port HBA
Brocade 815 Host Bus Adapter	8 Gbps 1-port HBA
Brocade 825 Host Bus Adapter	8 Gbps 2-port HBA
Brocade 48000 director	Director Chassis
Brocade 48000 director with FC4-16, FC4-32, and FC4-48[2] Blades	Director Chassis with 4 Gbps 16-FC port, 4 Gbps 32-FC port, and 4 Gbps 48-FC port
Brocade 48000 director with FR4-18i[1] Blades	Director Chassis with 4 Gbps router, extension blades
Brocade 48000 director with FC4-16IP[2] Blades	Director Chassis with 4 Gbps 8-FC port and 8 GbE iSCSI blades
Brocade 48000 director with FC10-6[4] Blades	Director Chassis with 10 Gbps 6-port ISL blades
Brocade DCX[7, 12, 13]	384-port Backbone Chassis
Brocade DCX[7] with FC8-16, FC8-32, and FC8-48 Blades	384-port Backbone Chassis with 8 Gbps 16-FC port, 8 Gbps 32-FC port, and 8 Gbps 48-FC port blades
Brocade DCX[7] with FR4-18i Blades	384-port Backbone Chassis with 4 Gbps Router, Extension blade
Brocade DCX with FC10-6 Blades	384-port Backbone Chassis with FC 10 - 6 ISL Blade
Brocade DCX[8] with FS8-18 Blades	384-port Backbone Chassis with Encryption Blade
Brocade DCX[11] with FX8-24 Blades	384-port Backbone Chassis with 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade
Brocade DCX[11] with FCoE10-24 Blades	384-port Backbone Chassis with 8 Gbps 24-port FCoE blade
Brocade DCX-4S[7, 12]	192-port Backbone Chassis
Brocade DCX-4S[9] with FC8-16, FC8-32, and FC8-48 Blades	192-port Backbone Chassis with 8 Gbps 16-FC port, 8 Gbps 32-FC port, and 8 Gbps 48-FC port blades
Brocade DCX-4S[9] with FR4-18i Blades	192-port Backbone Chassis with 4 Gbps Router, Extension blade
Brocade DCX-4S[9] with FC10-6 Blades	192-port Backbone Chassis with FC 10 - 6 ISL Blade
Brocade DCX-4S[9] with FS8-18 Blades	192-port Backbone Chassis with Encryption Blade
Brocade DCX-4S[11] with FX8-24 Blades	192-port Backbone Chassis with 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade
Brocade DCX-4S[11] with FCoE10-24 Blades	192-port Backbone Chassis with 8 Gbps 24-port FCoE blade
Brocade Encryption Switch[8]	8 Gbps Encryption Switch
FS8-18 Encryption Blade	Encryption Blade
FA4-18 Application Platform Blade	Application Platform Blade
FC8-16 Blade	FC 8 GB 16-port Blade

TABLE 1 Supported Hardware

Device Name	Terminology used in documentation
FC8-32 Blade	FC 8 GB 32-port Blade
FC8-48 Blade	FC 8 GB 48-port Blade
FC10-6 Blade	FC 10 - 6 ISL Blade
FCoE10-24 Blade	10 Gig FCoE port Blade
FX8-24 Blade[12, 13]	8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension Blade
M4700F Fabric Switch[12]	32-Port, 4 Gbps Switch
M6140 Director[12]	140-Port Director
Mi10K Director[12]	256-Port Director

1 Platform requires Fabric OS v5.1.0 or later
2 Platform requires Fabric OS v5.2.0 or later
3 Platform requires Fabric OS v5.2.1 or later
4 Platform requires Fabric OS v5.3.0 or later
5 Platform requires Fabric OS v5.3.1 or later
6 Platform requires Fabric OS v6.1.0 or later
7 Platform requires Fabric OS v6.0.0 or later
8 Platform requires Fabric OS v6.1.1_enc or later
9 Platform requires Fabric OS v6.2.0
10 Platform requires Fabric OS v6.1.2_CEE
11 Platform requires Fabric OS v6.3.0 or later
12 Professional Edition can discover, but not manage this Device. Use the device's Element Manager, which can be launched from the Connectivity Map, to manage the device. This device cannot be used as a Seed switch.
13 Professional Plus Edition can discover, but not manage this Device. Use the device's Element Manager, which can be launched from the Connectivity Map, to manage the device. This device cannot be used as a Seed switch.

What's new in this document

The following changes have been made since this document was last released:

- Information that was added:
  - HBA configuration
  - HBA discovery
  - CEE/FCoE configuration
  - Active sessions
  - Icons legend
  - Port Auto Disable
  - Upload Failure Data Capture
  - SNMP Informs
  - Allow/Prohibit Matrix - save as, copy, and manual add
  - FCiP - add and edit tunnels, select switch, add and edit FCiP circuit (IPv4 and IPv6)

- Port properties - GigE and FCiP tunnels tabs
- Properties - device properties, host, and virtual machines tab
- Zoning - set change limits
- TI Zone Properties
- Technical Support for hosts

- Information that was changed:
  - Discovery - Add Fabric, Address Properties
  - Options - Display and Memory Allocation
  - FICON Merge
  - Allow/Prohibit Matrix configure
  - FCiP - Advance Settings
  - Resource Groups
  - Performance - Additional measures
- Information that was deleted:
  - None.

For further information about new features and documentation updates for this release, refer to the release notes.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
`code` text	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, switchShow. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

Key terms

For definitions specific to Brocade and Fibre Channel, see the *Brocade Glossary*.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Linus Torvalds	Linux
Microsoft Corporation	Windows, Windows NT, Internet Explorer
Netscape Communications Corporation	Netscape
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover
Sun Microsystems, Inc.	Sun, Solaris, Sun Fire, Sun Ultra, Java Plug-in
The Open Group	UNIX
VMware, Inc.	VMware

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade resources

To get up-to-the-minute information, go to *http://my.brocade.com* and register at no cost for a user ID and password.

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

http://www.amazon.com

White papers, online demos, and data sheets are available through the Brocade Web site at:

http://www.brocade.com/products-solutions/products/index.page

For additional Brocade documentation, visit the Brocade Web site:

http://www.brocade.com

Release notes are available on the Brocade Connect Web site and are also bundled with the Fabric OS firmware.

Other industry resources

For additional resource information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

http://www.fibrechannel.org

Getting technical help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. DCFM Serial Number

   To obtain the DCFM serial number, select **Help > License**. The **DCFM License** dialog box displays.

2. General Information

   - Switch model
   - Switch operating system version
   - Error numbers and messages received
   - **supportSave** command output
   - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
   - Serial console and Telnet session logs
   - syslog message logs

3. Switch Serial Number

   The switch serial number and corresponding bar code are provided on the serial number label, as illustrated below.:

   The serial number label is located as follows:

   - *Brocade 200E*—On the nonport side of the chassis
   - *Brocade 300, 4100, 4900, 5100, 5300, 7500, 8000, and Brocade Encryption Switch*—On the switch ID pull-out tab located inside the chassis on the port side on the left
   - *Brocade 5000*—On the switch ID pull-out tab located on the bottom of the port side of the switch
   - *Brocade 7600*—On the bottom of the chassis
   - *Brocade 48000*—Inside the chassis next to the power supply bays
   - *Brocade DCX*—On the bottom right on the port side of the chassis

4. World Wide Name (WWN)

   Use the **wwn** command to display the switch WWN.

   If you cannot use the **wwn** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

1

User interface overview

In this chapter

- User interface components 1
- Icon legend. 16
- Shortcut menus 19
- Feature-to-firmware requirements 31
- Accessibility features for the Management application 33

User interface components

The Management application provides easy, centralized management of the SAN, as well as quick access to all product configuration applications. Using this application, you can configure, manage, and monitor your networks with ease.

The Management application's main window contains a number of areas. The following graphic illustrates the various areas, and descriptions of them are listed below.

NOTE
Some panels may be hidden by default. To view all panels, select **View > Show Panels > All Panels**, or press **F12**.

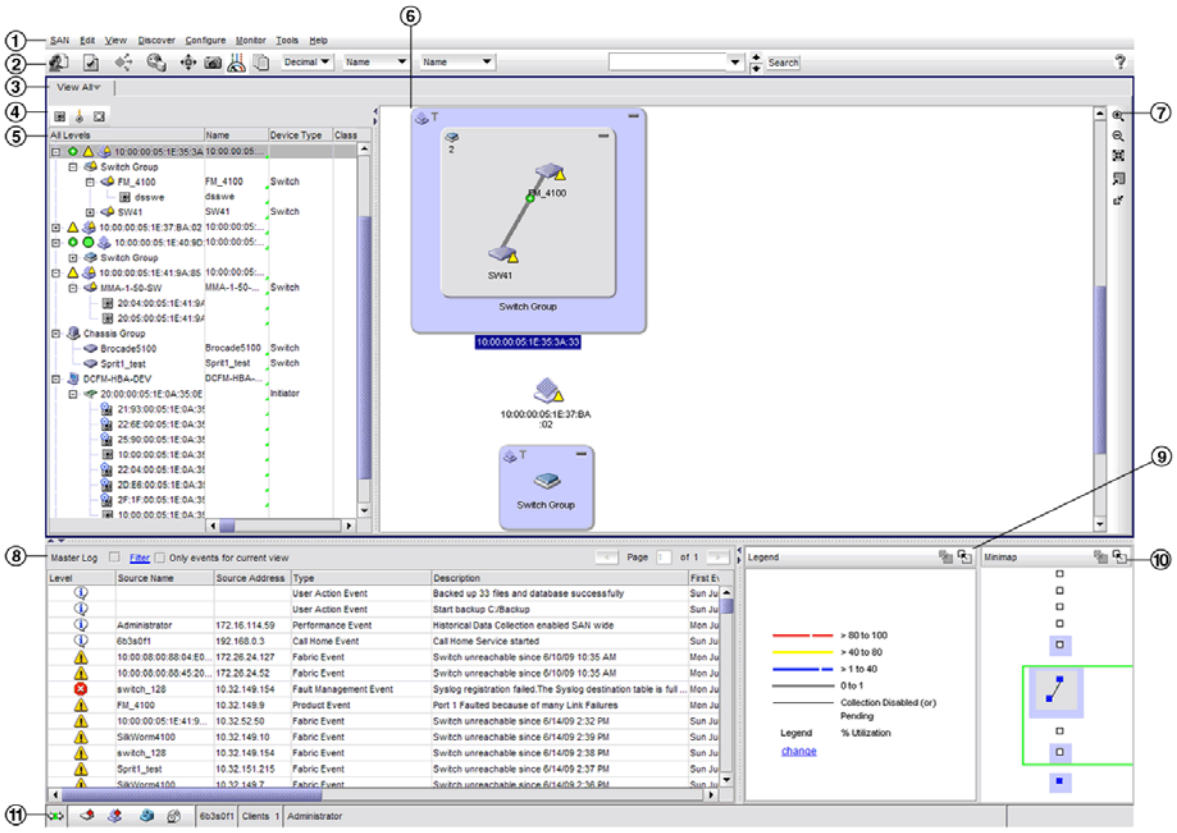


FIGURE 1 **Main Window**

1. **Menu Bar.** Lists commands you can perform on the SAN.
2. **Toolbar.** Provides buttons that enable quick access to dialog boxes and functions.
3. **View All tab.** Displays the Master Log, Minimap, Connectivity Map (topology), and Product List. For more information, refer to the View All tab.
4. **Port Display buttons.** Provides buttons that enable quick access to configuring how ports display. For more information, refer to "Port Display buttons" on page 11.
5. **Product List.** Lists the devices discovered in the SAN.
6. **Connectivity Map.** Displays the SAN topology, including discovered and monitored devices and connections.
7. **Toolbox.** Provides tools for viewing the Connectivity Map.
8. **Master Log.** Displays all events that have occurred on the SAN.
9. **Utilization Legend.** (Enterprise edition only) Indicates the percentage ranges represented by the colored, dashed lines on the Connectivity Map. Only displays when you select **Monitor > Performance > View Utilization** or click the **Utilization** icon on the toolbar.
10. **Minimap.** Displays a "bird's-eye" view of the entire SAN.
11. **Status Bar.** Displays data regarding the Server, connection, device, and fabric.

Menu bar

The menu bar is located at the top of the main window. The following table outlines the many functions available on each menu.

TABLE 2 Menu Bar

Menu	Command	Command Options
SAN Menu		
	Users. (Professional Plus and Enterprise Edition Only) Select to configure users and user groups.	
	Active Sessions. Select to display the active Management application sessions.	
	Server Properties. Select to display the Server properties.	
	Options. Select to configure the Management application options.	
	Exit. Select to close the Management Client.	
Edit Menu		
	Copy. Select to copy information and move it to another location.	
	Show Connections. Select to show connections in a group.	
	Select All. Select to select all objects in the Connectivity Map and Product List.	
	Properties. Select to display the selected objects properties.	
View Menu		
	Show Panels. Select to select which panels to display.	
		All Panels. Select to show all panels.
		Connectivity Map. Select to only show the connectivity map.
		Product List. Select to only show the Product List.
		Master Log. Select to only show the Master Log.
	Manage View. Select to set up the Management application view.	
		Create View. Select to create a new view.
		Display View. Select to display by View All or by a view you create.
		Levels. Select to display by All Levels, Products and Ports, Product Only, or Ports Only.
		Copy View. Select to copy a view.
		Delete View. Select to delete a view.
		Edit View. Select to edit a view.
	Zoom. Select to configure the zoom percentage.	

TABLE 2 Menu Bar

Menu	Command	Command Options
	Show. Select to determine what products display.	
		Fabrics Only. Select to display only fabrics.
		Groups Only. Select to display only groups.
		All Products. Select to display all products.
		All Ports. Select to display all ports.
	Enable Flyover Display/Device Tips. Select to enable flyover display.	
	Show Ports. Select to show utilized ports on the selected device.	
	Connected End Devices. Select to show or hide all connected end devices.	
		Hide All. Select to hide all connected end devices.
		Show All. Select to show all connected end devices.
		Custom. Select to set a custom display for all connected end devices.
	Map Display. Select to customize a group's layout to make it easier to view the SAN and manage its devices.	
	Domain ID/Port #. Select to set the display domain IDs and port numbers in decimal or hex format.	
		Decimal. Select to display all domain IDs and port numbers in decimal format.
		Hex. Select to display all domain IDs in hex format.
	Product Label. Select to configure which product labels display.	
		Name. Select to display the product name as the product label.
		Node WWN. Select to display the node name as the product label.
		IP Address. Select to display the IP Address (IPv4 or IPv6 format) as the product label.
		Domain ID. Select to display the domain ID as the product label.
	Port Label. Select to configure which port labels display.	
		Name. Select to display the name as the port label.
		Port #. Select to display the port number as the port label.
		Port Address. Select to display the port address as the port label.
		Port WWN. Select to display the port world wide name as the port label.

TABLE 2 Menu Bar

Menu	Command	Command Options
		User Port #. Select to display the user port number as the port label.
		Slot/Port #. Select to display the slot/port number as the port label.
	Port Display. Select to configure how ports display.	
		Occupied Product Ports. Select to display the ports of the devices in the fabrics (present in the Connectivity Map) that are connected to other devices.
		UnOccupied Product Ports. Select to display the ports of the devices (shown in the Connectivity Map) that are not connected to any other device.
		Attached Ports. Select to display the attached ports of the target devices.
		Switch to Switch Connections. Select to display the switch-to-switch connections.
Discover Menu		
	Setup. Select to set up Discovery.	
	Server Port Mapping. (Professional Plus and Enterprise Edition Only) Select to manually map ports to a server.	
	Storage Port Mapping. (Professional Plus and Enterprise Edition Only) Select to manually map Storage Ports to a Storage Device or other Storage Ports.	
Configure Menu		
	Element Manager. Select to configure a selected device.	
		Hardware. Select to the Element Manager or Web Tools application for the selected device.
		Ports. Select to launch Web Tools for the selected device.
		Admin. Select to launch Web Tools for the selected device.
		Router Admin. Select to launch Web Tools for the selected device.
	FC Switch. Select to manage a selected device.	
		Save. Select to save device configurations to the repository.
		Restore. Select to restore device configurations from the repository.
		Configuration Repository. (Professional Plus and Enterprise Edition Only) Select to manage device configurations from the repository.
		Schedule Backup. (Professional Plus and Enterprise Edition Only) Select to schedule configuration backup.

TABLE 2 Menu Bar

Menu	Command	Command Options
		Replicate. (Professional Plus and Enterprise Edition Only) Select to replicate the switch Configuration or Security.
		Swap Blades. (Professional Plus and Enterprise Edition Only) Select to swap blades.
	CEE Switch. Select to manage a selected switch.	
		CEE. Select to manage a CEE switch, port, or link aggregation group (LAG).
		FCoE. Select to manage an FCoE port.
	Firmware Management. Select to download firmware to devices.	
	Routing. Select to manage a selected router.	
		Configuration. (Professional Plus and Enterprise Edition Only) Select to view the R_Ports on a router.
		Domain IDs. (Professional Plus and Enterprise Edition Only) Select to configure the router domain IDs.
	Logical Switches. (Professional Plus and Enterprise Edition Only) Select to configure logical switches for your SAN.	
	Encryption. (Professional Plus and Enterprise Edition Only) Select to configure encryption for your SAN.	
	Zoning. Select to configure zones.	
		Fabric. Select to configure fabric zones.
		LSAN. (Professional Plus and Enterprise Edition Only) Select to configure LSAN zones.
		Set Change Limits. Select to set zone limits for zone activation.
	Names. Select to provide familiar simple names to products and ports in your SAN.	
	FCIP Tunnels. Select to connect to remote fabrics.	
	High Integrity Fabric. (Professional Plus and Enterprise Edition Only) Select to activate the following on M-EOS and Fabric OS devices: • On M-EOS switches, HIF activates fabric binding, switch binding, insistent domain ID and RSCNs. • On Fabric OS switches, HIF activates SCC policy, sets Insistent Domain ID and sets Fabric Wide Consistency Policy for SCC in tolerant mode.	
	Fabric Binding. (Professional Plus and Enterprise Edition Only) Select to configure whether switches can merge with a selected fabric, which provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.	

TABLE 2 Menu Bar

Menu	Command	Command Options
	Port Fencing. (Professional Plus and Enterprise Edition Only) Select to configure port fencing to protect your SAN from repeated operational or security problems experienced by ports.	
	Port Auto Disable. Select to configure port auto disable flag on individual FC_ports or all ports on a selected device, as well as unblock currently blocked ports.	
	FICON. (Enterprise Edition Only) Select to configure FICON.	
		Configure Fabric. Select to configure cascaded FICON from the selected fabric.
		Merge Fabrics. Select to merge the selected fabrics.
	Allow/Prohibit Matrix. (Enterprise Edition Only) Select to allow FICON users to configure an Allow/Prohibit Matrix table. You can select any matrix tables and compare them either vertically or horizontally.	
	Port Groups. (Professional Plus and Enterprise Edition Only) Select to configure a group of ports from one or more switches within the same fabric.	
	FC Troubleshooting. Select to troubleshoot your SAN.	
		Trace Route. Select to view the route information between two device ports.
		Device Connectivity. Select to view the connectivity information for two devices.
		Fabric Device Sharing. (Professional Plus and Enterprise Edition Only) Select to determine if the selected fabrics are configured to share devices.
	IP Troubleshooting. Select to troubleshoot your IP.	
		Ping. Select to perform a zoning check between the selected device port WWNs.
		Trace Route. (Professional Plus and Enterprise Edition Only) Select to view the route information from a source port on the local device to a destination port on another device.
		Performance. (Professional Plus and Enterprise Edition Only) Select to view IP performance between two devices.
	List Zone Members. (Professional Plus and Enterprise Edition Only) Select to display all members in a zone.	
Monitor Menu.		
	Performance. Select to monitor SAN devices.	
		View Utilization. (Professional Plus and Enterprise Edition Only) Select to display connection utilization.

TABLE 2 Menu Bar

Menu	Command	Command Options
		HIstorical Data Collection. (Professional Plus and Enterprise Edition Only) Select to monitor historical data on the entire SAN or selected parts of the SAN. You can also disable historical data monitoring.
		End-to-End Monitors. (Professional Plus and Enterprise Edition Only) Select to monitor end-to-end connections.
		Configure Thresholds. (Professional Plus and Enterprise Edition Only) Select to monitor thresholds.
		Clear Counters. Select to clear all port statistics counters.
		Top Talkers. (Professional Plus and Enterprise Edition Only) Select to monitor performance through a real-time list of top conversations for a switch or port along with related information.
		Real-Time Graph. Select to monitor performance through a graph, which displays transmit and receive data. The graphs show real-time data.
		Historical Graph. (Professional Plus and Enterprise Edition Only) Select to monitor a performance through a graph, which displays transmit and receive data. The graphs show historical data.
		Historical Report. (Professional Plus and Enterprise Edition Only) Select to monitor a performance through a table, which displays transmit and receive data. The table shows historical data.
	Technical Support. Select to configure technical support data for Fabric OS devices.	
		SupportSave. (Fabric OS devices only) Select to configure technical support data collection.
		Upload Failure Data Capture. Select to configure capture failure data for Fabric OS devices.
		View Repository. Select to view repository data.
	Event Policies. Select to configure event policies.	
	Event Notification. Select to configure the Management application to send event notifications at specified time intervals.	
		E-mail. Select to configure the Management application to send event notifications through e-mail.
		Call Home. (Professional Plus and Enterprise Edition Only) Select to configure the Management Server to automatically dial-in to or send an E-mail to a support center to report system problems.
	SNMP Setup. Select to configure SNMP traps.	
	Syslog Configuration. Select to configure Syslog for the management server.	
	Logs. Select to display logs.	

TABLE 2 Menu Bar

Menu	Command	Command Options
		Audit. Select to display a history of user actions performed through the application (except login/logout).
		Event. Select to display errors related to SNMP traps and Client-Server communications.
		Fabric. Select to display the events related to the selected fabric.
		FICON. Select to display the FICON events related to the selected device or fabric.
		Product Status. Select to display operational status changes of managed products.
		Security. Select to display security information.
		Syslog. Select to display Syslog events related to the selected device or fabric.
	Reports. Select to generate reports about the SAN.	
		Generate. Select to determine which reports to run.
		View. Select to view reports through the application or through an internet browser.
	Track Fabric Changes. (Professional Plus and Enterprise Edition Only) Select to track fabric changes on the selected fabric.	
	Accept Change(s). (Professional Plus and Enterprise Edition Only) Select to accept changes to the selected fabric.	
	Port Connectivity. Select to view port connectivity on the selected device.	
	Port Optics (SFP). Select to display the properties associated with a selected small form-factor pluggable (SFP) transceiver on the selected device.	
	Events. Select to display all events triggered on the selected device.	
Tools Menu		
	Setup. (Professional Plus and Enterprise Edition Only) Select to set up the applications that display on the **Tools** menu.	
	Product Menu. Select to access the tools available on a device's shortcut menu.	
	Tools List (determined by user settings). Select to open a software application. You can configure the **Tools** menu to display different software applications. Recommended tools to include in this menu include an internet browser, the command prompt application, and Notepad.	
Help Menu		
	Contents. Select to open the Online Help.	

TABLE 2 Menu Bar

Menu	Command	Command Options
	Find. Select to search the Online Help.	
	About <*Management_Application_Name*>**.** Select to view the application information, such as the company information and release number.	

Toolbar

The toolbar is located at the top of the main window and provides icons to perform various functions (Figure 2).

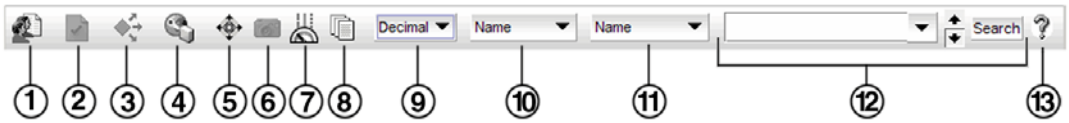


FIGURE 2 The Toolbar

The icons on your toolbar will vary based on the licensed features on your system.

1. **Users.** Displays the **Server Users** dialog box. Use to configure users, user groups, and permissions.
2. **Properties.** Displays the **Properties** dialog box of the selected device or fabric. Use to view or edit device or fabric properties.
3. **Launch Element Manager.** Launches the Element Manager of the selected device. Use to configure a device through its Element Manager.
4. **Discover Setup.** Displays the **Discover Setup** dialog box. Use to configure discovery.
5. **Zoning.** Displays the **Zoning** dialog box. Use to configure zoning.
6. **Track Fabric Changes.** Select to turn track fabric changes off for the selected device or group.
7. **View Utilization.** Displays or hides the utilization legend.
8. **View Report.** Displays the **View Reports** dialog box. Use to view available reports.
9. **Domain ID/Port #.** Use to set the domain ID or port number to display as decimal or hex in the Connectivity Map.
10. **Product Label.** Use to set the product label for the devices in the Connectivity Map.
11. **Port Label.** Use to set the port label for the devices in the Connectivity Map.
12. **Product List Search.** Use to search for a device in the product list.
13. **Help.** Displays the Online Help.

View All tab

The **View All** tab displays the Master Log, Utilization Legend, Minimap, Connectivity Map (topology), and Product List.

To open all areas of the **View** window, select **View > Show Panels > All Panels** or press **F12**.

You can change the default size of the display by placing the cursor on the divider until a double arrow displays. Click and drag the adjoining divider to resize the window. You can also show or hide an area by clicking the left or right arrow on the divider.

Port Display buttons

The Port Display buttons (Figure 3) are located at the top left side of the **View** window and enable you to configure how ports display. You have the option of viewing connected (or occupied) product ports, unoccupied product ports, or attached ports.

NOTE
Occupied/connected ports are those that originate from a device, such as a switch. Attached ports are ports of the target devices that are connected to the originating device.

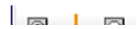


FIGURE 3 Port Display buttons

1. **Occupied Product Ports**. Displays the ports of the devices in the fabrics (present in the connectivity map) that are connected to other devices.
2. **Unoccupied Product Ports**. Displays the ports of the devices (shown in the connectivity map) that are not connected to any other device.
3. **Attached Ports**. Displays the attached ports of the target devices.

Product List

The Product List, located on the **View All** tab, displays an inventory of all discovered devices and ports. The Product List is a quick way to look up product and port information, including serial numbers and IP addresses.

To display the Product List, select **View > Show Panels > Product List** or press **F9**.

You can edit information in the Product List by double-clicking in a field marked with a green triangle. You can sort the Product List by clicking a column heading.

The following columns (presented here in alphabetical order) are included in the Product List.

- **All Levels.** Displays all discovered fabrics, groups, devices, and ports as both text and icons. Also, displays the status of the fabrics, groups, devices, and ports. For a list of icons that display in the All Levels column, refer to the following tables:
  - "Product icons" on page 16
  - "Group icons" on page 17
  - "Port icons" on page 17
  - "Product status icons" on page 18
- **Attached Port #.** Displays the number of the attached port.

- **BB Credit.** Displays the BB Credit for the product.
- **Class.** Displays the class to which the product belongs.
- **Contact.** Displays the name of the person or group you should contact about the product. This field is editable at the fabric and device level.
- **Description.** Displays the description of the product. This field is editable at the fabric and device level.
- **Device Type.** Displays the type of device.
- **Domain ID.** Displays the Domain ID for the product in the format xx(yy), where xx is the normalized value and yy is the actual value on the wire.
- **FC Address.** Displays the Fibre Channel address of the port.
- **Firmware.** Displays the firmware version of the product. This field is editable at the device level.
- **IP Address.** Displays the IP address (IPv4 or IPv6 format) of the product. This field is editable at the device level.
- **Location.** Displays the physical location of the product. This field is editable at the fabric and device level.
- **Model.** Displays the model number of the product. This field is editable at the device level.
- **Name.** Displays the name of the product.
- **Port #.** Displays the number of the port.
- **Port Count.** Displays the number of ports on the product.
- **Port Type.** Displays the type of port (for example, expansion port, node port, or NL_port).
- **Protocol.** Displays the protocol for the device.
- **Serial #.** Displays the serial number of the product. This field is editable at the device level.
- **Speed Configured (Gbps).** Displays the actual speed of the port in Gigabits per second.
- **State.** Displays the port state.
- **Status.** Displays the status for the product.
- **Symbolic Name.** Displays the symbolic name for the product.
- **TAG.** Displays the tag number of the port.
- **Vendor.** Displays the name of the product's vendor.
- **WWN.** Displays the world wide name of the product.

Connectivity Map

The Connectivity Map, which displays in the upper right area of the main widow, is a grouped map that shows physical and logical connectivity of SAN components, including discovered and monitored devices and connections. These components display as icons in the Connectivity Map. For a list of icons that display in the Connectivity Map, refer to the following tables:

- "Product icons" on page 16
- "Group icons" on page 17
- "Product status icons" on page 18

The Management application displays all discovered fabrics in the Connectivity Map by default. To display a discovered Host in the Connectivity Map, you must select the Host in the Product List. You can only view one Host and physical and logical connections at a time.

Toolbox

The toolbox (Figure 4) is located at the top right side of the **View** window and provides tools to zoom in and out of the Connectivity Map, collapse and expand groups, and fit the topology to the window.

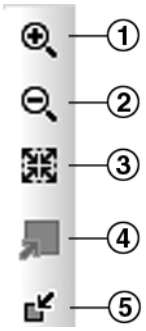


FIGURE 4 The Toolbox

1. **Zoom In.** Use to zoom in on the Connectivity Map
2. **Zoom Out.** Use to zoom out on the Connectivity Map.
3. **Fit in View.** Use to scale the map to fit within the Connectivity Map area.
4. **Expand.** Use to expand the map to show all ports in use on a device.
5. **Collapse.** Use to collapse the map to show only devices (hides ports).

Master Log

The Master Log, which displays in the lower left area of the main window, lists the events and alerts that have occurred on the SAN. If you do not see the Master Log, select **View > Show Panels > All Panels** or press **F5**.

You can configure the Management application to archive log files over 45 days old. For step-by-step instructions, refer to "Configuring event storage" on page 82.

The following fields and columns are included in the Master Log:

- **Level.** The severity of the event. For more information about events, refer to "Fault Management" on page 171. For a list of the event icons, refer to Table 7.
- **Source Name.** The product on which the event occurred.
- **Source Address.** The IP address (IPv4 or IPv6 format) of the product on which the event occurred.
- **Type.** The type of event that occurred (for example, client/server communication events).
- **Description.** A description of the event.
- **First Event Server Time.** The time and date the event first occurred on the server.
- **Last Event Server Time.** The time and date the event last occurred on the server.
- **First Event Product Time.** The time and date the event first occurred on the product.
- **Last Event Product Time.** The time and date the event last occurred on the product.
- **Operational Status.** The operational status of the product on which the event occurred.
- **Count.** The number of times the event occurred.

- **Module Name.** The name of the module on which the event occurred.
- **Message ID.** The message ID of the event.
- **Contributor.** The name of the contributor on which the event occurred.
- **Node WWN.** The world wide name of the node on which the event occurred.
- **Fabric Name.** The name of the fabric on which the event occurred.

Minimap

The Minimap, which displays in the lower right corner of the main window, is useful for getting a bird's-eye view of the SAN, or to quickly jump to a specific place on the Connectivity Map. To jump to a specific location on the Connectivity Map, click that area on the Minimap. A close-up view of the selected location displays on the Connectivity Map.

Use the Minimap to view the entire SAN and to navigate more detailed map views. This feature is especially useful if you have a large SAN.

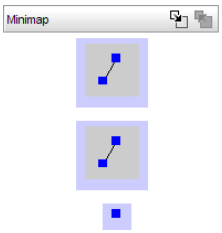


FIGURE 5 Minimap

Anchoring or floating the Minimap

You can anchor or float the Minimap to customize your main window.

- To float the Minimap and view it in a separate window, click the **Detach** icon ( ) in the upper right corner of the Minimap.
- To anchor the Minimap and return the Minimap to its original location on the main window, do one of the following steps:
  - Click the **Attach** icon ( ) in the upper right corner of the Minimap.
  - Click the **Close** icon ( ) in the upper right corner of the Minimap.
  - Double-click the logo in the upper left corner of the Minimap.
  - Click the logo in the upper left corner of the Minimap and select **Close** (**ALT** + **F4**).

Resizing the Minimap

On an anchored Minimap, place the cursor on the left border of the Minimap until a double-pointed arrow displays. Click and drag the adjoining divider.

On a floating Minimap, place the cursor on a border of the Minimap until a double-pointed arrow displays. Click and drag to change the window size.

Status bar

The status bar (Figure 6) displays at the bottom of the main window. The status bar provides a variety of information about the SAN and the application. The icons on the status bar change to reflect different information, such as the current status of products, fabrics, and backup.

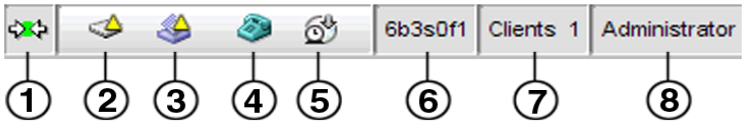


FIGURE 6 **Status Bar**

The icons on your status bar will vary based on the licensed features on your system.

1. **Connection Status.** Displays the Server-Client connection status.
2. **Product Status.** Displays the status of the most degraded device in the SAN. For example, if all devices are operational except one (which is degraded), the Product Status displays as degraded. Click this icon to open the **Product Status Log**.
3. **Fabric Status.** Displays the state of the fabric that is least operational, based on ISL status. The possible states are: operational, unknown, degraded or failed. Select a product or fabric from the Connectivity Map or Product List and click this icon to open the related **Fabric Log** (only available for persisted fabrics).
4. **Call-Home Status.** (Enterprise edition only) Displays a call home status icon when one or more fabrics are discovered, which allows you to determine the current call home status.
5. **Backup Status.** Displays a backup status icon, which allows you to determine the current backup status. Let the pointer pause on the backup status icon to display the following information in a tooltip.
   - **Backup in Progress icon.** Backup started at hh:mm:ss, in progress... *XX* files in <*directory_name*> are backed up.
   - **Countdown to Next Scheduled Backup icon.** Waiting for next backup to start.
   - **Backup Disabled icon.** Backup is disabled.
   - **Backup Failed icon.** Backup failed at hh:mm:ss mm/dd/yyyy.
6. **Server Name.** Displays the name of the Server to which you are connected.
7. **Total Users.** Displays the number of clients logged into the server.
8. **User's ID.** Displays the user ID of the logged in user.

Icon legend

Various icons are used to illustrate devices and connections in a SAN. The following tables list icons that display on the Connectivity Map and Product List.

Product icons

The following table lists the manageable SAN product icons that display on the topology. Fabric OS manageable devices display with blue icons and M-EOS manageable devices display with green icons. If a device is unmanageable it displays with gray icons. Some of the icons shown in Table 3 only display when certain features are licensed.

TABLE 3 Product Icons

Icon	Description	Icon	Description
	Fabric		Fabric OS Director
	Fabric OS Switch and Blade Switch		Fabric OS CEE Switch
	Fabric OS Router		Access Gateway (single-fabric connected)
	Access Gateway (multiple-fabric connected)		Storage
	M-EOS Switch		M-EOS Director
	iSCSI Target		iSCSI Initiator
	HBA		Unmanaged HBA
	CNA HBA		Host
	VM Host		Unmanaged Host
	Ethernet Cloud		

Group icons

The following table lists the manageable SAN product group icons that display on the topology.

TABLE 4 Group Icons

Icon	Description	Icon	Description
	Switch Group		Host Group
	Storage Group		Unknown Fabric Group
	Unmanaged Fabric Group		Chassis Group

Port icons

The following table lists the product status icons that display in the Product List.

TABLE 5 Port Icons

Icon	Description
	Occupied FC Port
	Unoccupied FC Port
	Attached FC Port
	Trunk (port group)
	IP and 10 GE Port
	Attached IP and 10 GE Port
	Attached-to-Cloud 10 GE Port
	Virtual Port
	Virtual FCoE Port
	Attached FCoE Port

Product status icons

The following table lists the product status icons that display on the topology.

TABLE 6 Product Status Icons

Icon	Status
No icon	Healthy/Operational
	Attention
	Degraded/Marginal
	Device Added
	Device Removed/Missing
	Down/Failed
	Routed In
	Routed Out
	Unknown/Link Down

Event icons

The following table lists the event icons that display on the topology and Master Log. For more information about events, refer to "Fault Management" on page 171.

TABLE 7 Event Icons

Event Icon	Description
	Informational
	Warning
	Error

Shortcut menus

You can use the Management application interface main menu to configure, monitor, and troubleshoot your SAN components. The instructions for using these features are documented in the subsequent chapters of this manual.

For each SAN component, you can optionally right-click the component and a shortcut menu displays. The table below details the command options available for each component.

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
FC Fabric or Backbone Fabric		
	Zoning	
	LSAN Zoning (Device Sharing)	Professional Plus and Enterprise Edition Only Only enabled for Backbone fabrics.
	Performance > End-to-End Monitors (Professional Plus and Enterprise Edition Only) Real-Time Graph Historical Graph (Professional Plus and Enterprise Edition Only) Historical Report (Professional Plus and Enterprise Edition Only)	
	Events	
	Configure FCIP Tunnels	Only launches the wizard when FCIP-capable switches are in the selected fabric.
	High Integrity Fabric	Professional Plus and Enterprise Edition Only
	Fabric Binding	Professional Plus and Enterprise Edition Only
	Router Configuration	Professional Plus and Enterprise Edition Only
	Routing Domain IDs	Professional Plus and Enterprise Edition Only
	Technical Support > Collect Data Upload Failure Data Capture View Repository	
	View > Port List Node List	
	Track Fabric Changes check box	Professional Plus and Enterprise Edition Only
	Accept Changes	Professional Plus and Enterprise Edition Only
	Connected End Devices > Hide All Show All Custom	
	Create Meta SAN View	Only available for Backbone fabrics.

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
	Create View Automatically	Automatically creates a view with the selected fabric. View name is same as the current label.
	Map Display	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Collapse or Expand	Only available from Connectivity Map
	Table > Copy '<*Fabric_Name*>' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Device Group		
	Servers	Only available for servers or host group.
	Zoning	Only available for switch group.
	Storage Port Mapping	Professional Plus and Enterprise Edition Only Only available for storage group.
	Map Display	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '<*Device_Name*> Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
	Collapse or Expand	Only available from Connectivity Map
	Properties	Only available for servers.
	Map Display	Only available for chassis group.
Fabric OS Switch/Chassis/Access Gateway		
	Element Manager > Hardware Ports Admin Router Admin	
	Configuration > Save Restore Schedule Backup (Professional Plus and Enterprise Edition Only) Replicate > Configuration (Professional Plus and Enterprise Edition Only) Security (Professional Plus and Enterprise Edition Only) Swap Blades	
	Firmware Management	
	Zoning	Does not display when switch is in a Core Switch group, Chassis group or Isolated device group, or when it is in Access Gateway mode.
	Allow / Prohibit Matrix	Enterprise Edition Only Only available for Fabric OS devices. Only enabled when the Fabric OS device is FICON-capable and has the Enhanced Group Management license.
	Technical Support > Collect Data Upload Failure Data Capture View Repository	
	Port Connectivity	
	Port Optics (SFP)	
	Port Fencing	Professional Plus and Enterprise Edition Only
	Performance > Clear Counters Real-Time Graph Historical Graph (Professional Plus and Enterprise Edition Only) Historical Report (Professional Plus and Enterprise Edition Only)	

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
	Events	
	Enable / Disable > Enable Disable	
	Telnet	
	Telnet through Server	
	<User-defined menu item>	Professional Plus and Enterprise Edition Only Configured in Setup Tools. May be more than one item.
	Setup Tools	Professional Plus and Enterprise Edition Only
	Product	Only enabled when the fabric is tracked, and the product is removed and joins another fabric.
	Other Ports > <Fabric Name 1> <Fabric Name 2>	Does not display when an Access Gateway mode device is attached to multiple fabrics.
	Accept Change	Professional Plus and Enterprise Edition Only Only enabled in tracked FC Fabrics. Only enabled when a plus or minus icon is present.
	Show Ports check box	
	Show Connections	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '<*Device_Name*> Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Core Switch		
	Element Manager	Only available from Product List.
	Enable/Disable Virtual Fabric (Fabric OS only)	Only available from Product List.

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
	Logical Switches > <*List_of_Logical_Switches*> (Fabric OS only)	Only available from Product List.
	Configuration > (Fabric OS only) Save Restore Schedule Backup (Professional Plus and Enterprise Edition Only) Replicate > Configuration (Professional Plus and Enterprise Edition Only) Security (Professional Plus and Enterprise Edition Only) Swap Blades	
	Firmware Management (Fabric OS only)	
	Events	
	Technical Support > (Fabric OS only) Collect Data Upload Failure Data Capture View Repository	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '<*Device_Name*> Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
HBA, iSCSI Host, and HBA Enclosure		
	Element Manager	Launches Element Manager for Brocade HBAs discovered using JSON agent. Launches blank window for unmanaged Brocade HBAs.
	Servers	Does not display for routed devices and discovered hosts.
	Server Port Mapping	Only available for Brocade, Emulex, and Qlogic HBAs.

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
	Performance > Real Time Graphs	Disabled when all ports are offline. Does not display for Node Origin and Routed instance in a routed fabric.
	Mapping Product	Only available for Brocade HBAs.
	LightPulse Utility/NT	Only available for Emulex devices. Launches with Origin in context for routed device.
	Emulex Configuration Tool	Only available for Emulex devices. Launches with Origin in context for routed device.
	SANSurfer	Only available for Qlogic HBAs.
	<User-defined menu item>	Configured in Setup Tools. May be more than one item.
	Host	Only available in Fabric view for managed HBAs.
	Setup Tools	Professional Plus and Enterprise Edition Only
	Show Ports	
	Show Connections	
	Fabric > Fabric1 Fabric2	Only available for HBAs under the Host node.
	Origin	Only available for HBAs under the Host node or devices routed in. Not available for enclosures.
	Destination	Only available for devices routed out. Not available for enclosures.
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Expand All	Only available from Product List.
	Collapse All	Only available from Product List.
	Properties	
Storage, iSCSI Storage, and Storage Enclosure		
	Storage Port Mapping	Professional Plus and Enterprise Edition Only Disabled for routed device.
	<User defined menu item>	
	Setup Tools	Professional Plus and Enterprise Edition Only
	Show Ports	
	Show Connections	

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
	Origin	Only available for devices routed in. Not available for enclosures.
	Destination	Only available for devices routed out. Not available for enclosures.
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '<*Device_Name*> Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Router Phantom Domains		
	Accept Change	Professional Plus and Enterprise Edition Only Only available for tracked FC Fabrics. Only enabled when a plus or minus icon is present.
	Show Connections	Displays as disabled because this component does not display in the Connectivity Map.
	Origin	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '<*Device_Name*> Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
	Properties	
Switch Port FC		
	Performance > Real-Time Graph Historical Graph (Professional Plus and Enterprise Edition Only) Historical Report (Professional Plus and Enterprise Edition Only)	
	Zoning	
	Enable / Disable > Enable Disable	
	Connected Port	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '<*Device_Name*> Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Collapse All	Only available from Product List.
	Properties	
HBA and iSCSI Initiator		
	Servers	Does not display for routed devices and discovered Hosts.
	Performance > Real Time Graphs	Disabled when all ports are offline.
	FC Security Protocol	Only available for Managed JSON HBA Ports. Only available when you have the Security Privilege.
	Zoning	
	List Zone Members	Professional Plus and Enterprise Edition Only
	Connected Port	

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '<*Device_Name*> Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
HBA Port		
	Servers	Does not display for routed devices and discovered Hosts.
	Performance > Real Time Graphs	Only available for occupied, managed ports. Disabled when all ports are offline.
	FC Security Protocol	Only available for Managed JSON HBA Ports. Only available when you have the Security Privilege.
	Zoning	
	List Zone Members	Professional Plus and Enterprise Edition Only
	Connected Port	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Expand All	Only available from Product List.
	Collapse All	Only available from Product List.
	Properties	
Storage Node		
	Show Ports	Does not display for routed devices and discovered Hosts.
	Show Connections	
Storage FC and iSCSI Storage port		
	Storage Port Mapping	Professional Plus and Enterprise Edition Only

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
	Zoning	
	List Zone Members	Professional Plus and Enterprise Edition Only
	Connected Port	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '<*Device_Name*> Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Giga-Bit Ethernet Port		
	Performance > Real-Time Graph	
	Modify	Launches Element Manager.
	IP Troubleshooting > Ping Trace Route Performance (Professional Plus and Enterprise Edition Only)	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
	Table > Copy '<*Device_Name*> Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Connection		
	Properties	
FCIP Tunnel		
	Properties	
Trunk		
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '<*Device_Name*> Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
White Area of the Connectivity Map		
	Zoom	
	Zoom In	
	Zoom Out	
	Map Display	
	Expand	
	Collapse	

TABLE 8 Component Shortcut Menus

Component	Menu/Submenu Commands	Comments
White Area of the Product List		
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	
	Table > Copy '<*Component*>' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	
Product List		
	Table > Copy '<*Component*>' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Some form of this shortcut menu is available for all tables in the Management interface.

Feature-to-firmware requirements

Use the following table to determine whether the Management application features are only available with a specific version of the Fabric OS firmware, M-EOS firmware, or both, as well as if there are specific licensing requirements.

TABLE 9 Feature-to-firmware

Feature	Fabric OS	M-EOS
Access Gateway (AG)	AG connected to Fabric OS devices requires firmware 6.1.1 or later.	AG connected to M-EOS devices requires firmware 9.9.2 or later.
Call Home (Professional Plus and Enterprise Edition Only)	Requires Fabric OS 5.2 or later for supportSave. Requires Fabric Watch license for SNMP traps.	Requires M-EOS and M-EOSn 9.6.X or later.
Discovery	Requires Fabric OS 5.0 or later for the seed switch in a pure Fabric OS fabric. Requires Fabric OS 6.0 or later for the seed switch in a mixed Fabric OS and M-EOS fabric.	Requires M-EOS 9.9.2 or later for the seed switch in a pure M-EOS fabric. Requires M-EOS and M-EOSn 9.6.X or later for discovery.
Encryption (Professional Plus and Enterprise Edition Only)	Requires Fabric OS 6.1.1_enc.	Not available.
Enhanced Group Management (Professional Plus and Enterprise Edition Only)	Requires Enhanced Group Management license.	Not available.
Fault Management	Requires Fabric OS 4.4 or later for SNMP traps	Requires M-EOS and M-EOSn 9.6.X or later.
Fabric Binding (Professional Plus and Enterprise Edition Only)	Requires Fabric OS 5.2 or later in a pure Fabric OS fabric. Requires Fabric OS 6.0 or later in a mixed Fabric OS and M-EOS fabric.	Requires M-EOS and M-EOSn 9.6.X or later.
FCIP Management	Requires Fabric OS 5.1 or later to modify. Requires Fabric OS 5.3 or later for FCIP tunnels. Requires FCIP license. Requires Fabric OS 6.0 or later to enable the FICON Emulation tab on the FCIP Tunnel Advanced Settings dialog box.	Not available.
FICON (Enterprise Edition Only)	Requires Fabric OS 5.2 or later for cascaded FICON. Requires Fabric OS 6.0 or later for advanced FICON. Requires Fabric OS 6.1.1 or later to configure multiple Prohibit Dynamic Connectivity Mask (PDCM) matrices. Requires FICON CUP license to allow CUP management features.	Only supports cascaded FICON configuration for mixed fabrics.
Firmware Management	Requires Fabric OS 5.0 or later. Requires Fabric OS 6.1.1 or later on 8G devices. Requires Fabric Management license. Requires Enhanced Group Management license to perform group actions.	Firmware download is only available through the Element Manager.
High Integrity Fabric	Requires Fabric OS 5.2 or later in a pure Fabric OS fabric. Requires Fabric OS 6.0 or later in a mixed Fabric OS and M-EOS fabric.	Requires M-EOS and M-EOSn 9.6.X or later.

TABLE 9 Feature-to-firmware

Feature	Fabric OS	M-EOS
Meta SAN	Requires Fabric OS 5.2 or later for FC router and router domain ID configuration. Requires Fabric OS 6.0 or later in a mixed Fabric OS and M-EOS fabric. Requires Integrated Routing license.	Not available.
Performance	Requires Fabric OS 5.0 or later for FC_ports, end-to-end monitors, and marching ants. Requires Fabric OS 5.3 or later for GE_ports and FCIP tunnels. Requires Fabric OS 6.2 or later for Top Talkers. Requires Advanced Performance Monitoring (APM) license for End-to-end Monitoring and Top Talkers. Requires Enhanced Group Management license for HIstorical graphs and tables. Requires Fabric Watch license for Performance thresholds.	Requires M-EOS and M-EOSn 9.6.X or later for FC_ports and marching ants.
Port Fencing (Professional Plus and Enterprise Edition Only)	Requires Fabric OS 6.2 or later.	Requires M-EOS and M-EOSn 9.6.X or later.
Security Management	Requires Fabric OS 5.2 and later for SCC Policy. Requires Fabric OS 5.2 and later for DCC Policy. Requires Fabric OS 5.3 and later for IP Filter Policy. Requires Fabric OS 6.0 and later for AD/LDAP Server Configuration. Requires Fabric OS 5.0 and later for RADIUS Server Configuration.	Not available.
Technical Support Data Collection	Requires Fabric OS 5.2 or later.	Data collection support is only available through the Element Manager.
Troubleshooting and Diagnostics	Requires Fabric OS 5.2 or later.	Not available.
Virtual Fabrics (Professional Plus and Enterprise Edition Only)	Requires at least one Virtual Fabrics-enabled physical chassis running Fabric OS 6.2 or later.	Virtual Fabric configuration is only available through the Element Manager.
Zoning	Requires Fabric OS 5.0 or later for pure Fabric OS fabrics. Requires Fabric OS 6.0 or later for McDATA Fabric Mode. Requires Adaptive Networking license for Quality of Service zones.	Requires M-EOS and M-EOSn 9.6.X or later for a pure M-EOS fabric and Mixed Fabrics in Interopmode 3.

Accessibility features for the Management application

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

The following list includes the major accessibility features in the Management application:

- Keyboard shortcuts
- Look and Feel

Keyboard shortcuts

You can use the keystrokes shown in Table 10 to perform common functions.

NOTE
To open a menu using keystrokes, press ALT plus the underlined letter. To open a submenu, open the menu, then press the key for the underlined letter (SHIFT plus letter for capitals) of the submenu option.

TABLE 10 Keyboard Shortcuts

Menu Item or Function	Keyboard Shortcut
All Panels	F12
Collapse	CTRL + L
Command Tool	SHIFT + F4
Connectivity Map	F7
Copy	CTRL + C
Cut	CTRL + X
Delete	Delete
Delete All	CTRL +Delete
Expand	CTRL + E
Help	F1
Internet Explorer	SHIFT + F2
Master Log	F5
FireFox	SHIFT + F1
Paste	CTRL + V
Product List	F9
Properties	Alt-Enter
Select All	CTRL + A
Show Ports	F4
SSH	Shift-F5
View Utilization	CTRL + U

TABLE 10 Keyboard Shortcuts

Menu Item or Function	Keyboard Shortcut
Zoom In	CTRL + NumPad+
Zoom Out	CTRL + NumPad-

Look and Feel

You can configure the Management application to mimic your system settings as well as define the size of the font.

'Look' refers to the appearance of graphical user interface widgets and 'feel' refers to the way the widgets behave.

The Management application currently uses the '<*Management_Application_Name*> Default Look and Feel' for some of the components (for example, Layout, Minimap, and so on) and the "Java Metal Look and Feel" for others.

Setting the look and feel

NOTE
Setting the look and feel is only supported on Windows systems.

The following table details the Management application components that change when you set the look and feel as well as those components that do not change.

TABLE 11 System changes

Components Affected	Components Not Affected
All Java native components with Metal Look And Feel are affected.	The Connectivity map does not change when devices are present. You must change the theme using the map display settings (**View > Map Display**).
The Menu bar, Tool bar, Status bar, as well as all tables and dialog boxes are affected.	All icons and images are not affected.
Layout is affected only when it is empty.	The Minimap is not affected.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Look and Feel** in the **Category** list.

3. Choose from one of the following options:

   - Select **Default** to configure the look and feel back to the Management application defaults.
   - Select **System** to configure the Management application to have the look and feel of your system.

     This changes the look and feel for the components that use 'Java Metal Look and Feel'. For example, if you have your system display color scheme set to 'High Contrast #1', then the Management application will be set to 'High Contrast #1'. Font size of the components is not affected by theme changes.

4. Click **Apply** or **OK** to save your work.
5. Click **OK** on the message.

NOTE
Changes do not take affect until after you restart the client.

Changing the font size

The **Options** dialog box enables you to change the font size for all components including the Connectivity map of the Management application interface.

Font size changes proportionately in relation to the system resolution. For example, if the system resolution is 1024 x 768, the default font size would be 8 and large font size would be 10.

1. Select **SAN > Options**.

   The **Options** dialog box displays.
2. Select **Look and Feel** in the **Category** list.
3. Select one of the following options from the **Font Size** list:
   - Select **Default** to return to the default font size.
   - Select **Small** to change the font to a smaller font size.
   - Select **Large** to change the font to a larger font size.

     NOTE
     Changing the font size to **Large** may cause the interface components (for example, text and button labels) to display incorrectly.
4. Click **Apply** or **OK** to save your work.
5. Click **OK** on the message.

NOTE
Changes do not take affect until after you restart the client.

Chapter

2

Discovery

In this chapter

- Fabric discovery overview 37
- Host discovery 44
- Viewing the discovery state. 50
- Fabric monitoring. 51
- Seed switch 53

Fabric discovery overview

Discovery is the process by which the Management application contacts the devices in your SAN. When you configure discovery, the application discovers products connected to the SAN. The application illustrates each product and its connections on the Connectivity Map (topology).

When you discover a fabric, the Management application checks to confirm that the seed switch is running a supported Fabric OS version in the fabric, and if it is not, the Management application prompts you to select a new seed switch.

NOTE
Discovery of a Secure Fabric OS fabric in strict mode is not supported.

For a Fabric OS fabric, the seed switch must be the primary Fabric Configuration Server (FCS). If you use a non-primary FCS to discover the fabric, the Management application displays an error and will not allow the discovery to proceed. If the Management application has already discovered the fabric, but afterward you create the FCS policy and the seed switch is not a primary FCS, an event is generated during the next poll.

The Management application cannot discover a fabric that is in the process of actively configuring to form a fabric. Wait until the fabric is formed and stable, then re-attempt the fabric discovery.

After fabric discovery successfully completes, all clients are updated to display the newly discovered fabric.

During fabric discovery, if you have defined IPv6 IP addresses for the switch, the Management application remembers the IP address only. If the switch has a DNS name that you have defined, the Management application can remember the DNS name and use that.

NOTE
Professional edition can discover only 1 fabric.

NOTE
Professional edition can discover, but not manage M-EOS devices or the Backbone chassis. Use the device's Element Manager, which can be launched from the Connectivity Map, to manage the device. This device cannot be used as a Seed switch.

FCS policy and seed switches

The Management application requires that the seed switch is the primary Fabric Content Service (FCS) switch at the time of discovery.

Setting time on the fabric will set the time on the primary FCS switch, which will then distribute the changes to other switches.

When FCS Policy is defined, **ConfigDownload** is allowed only from the primary FCS switch, but Management application does not check at the time of download that the switch is the primary FCS Switch.

NOTE
Switches running in Access Gateway mode cannot be used as the seed switch.

NOTE
The Backbone Chassis cannot be used as a seed switch.

Discovering fabrics

NOTE
Fabric OS devices must be running Fabric OS 5.0 or later. M-EOS devices must be running M-EOS 9.6 or later.

NOTE
Only one copy of the application should be used to monitor and manage the same devices in a subnet.

To discover specific IP addresses or subnets, complete the following steps.

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.

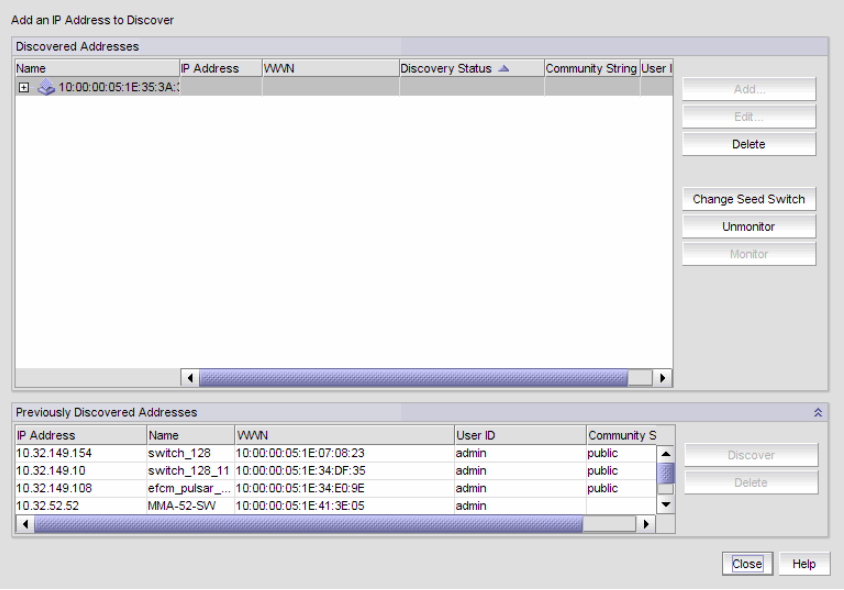


FIGURE 7 **Discover Setup Dialog Box**

2. Click **Add Fabric** to specify the IP addresses of the devices you want to discover.

   The **Address Properties** dialog box displays.

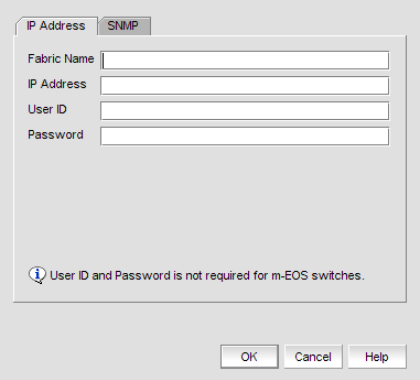


FIGURE 8 **Address Properties Dialog Box (IP Address tab)**

3. Enter a name for the fabric in the **Fabric Name** field.
4. Enter an IP address for a device in the **IP Address** field.

   For seed switch requirements, refer to "Seed switch requirements" on page 54.

NOTE
The Backbone Chassis cannot be used as a seed switch.

NOTE
Professional and Professional Plus editions cannot manage the Backbone Chassis. Professional edition cannot manage pure M-EOS fabrics.

NOTE
Professional edition can discover only 1 fabric.

5. If a user ID and password are required, enter them in the **User ID** and **Password** fields.
6. Click the **SNMP** tab (Figure 9).

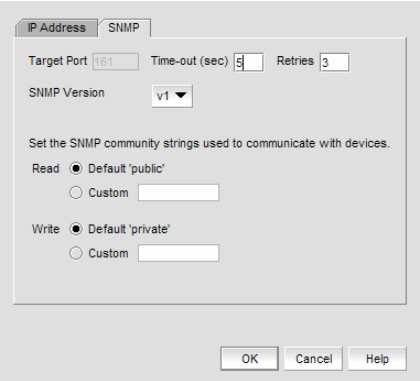


FIGURE 9 **Address Properties Dialog Box (SNMP - v1 tab)**

7. Enter the target port in the **Target Port** field.

8. Enter the duration (in seconds) after which the application times out in the **Time-out (sec)** field.
9. Enter the number of times to retry the process in the **Retries** field.
10. Select the SNMP version from the **SNMP Version** list.
    - If you selected v1, continue with step 11.
    - If you select v3, the SNMP tab displays the v3 required parameters. Go to step 15.
11. Specify the **Read** option by selecting **Default 'public'** or **Custom**.
12. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.
13. Specify the **Write** option by selecting **Default 'private'** or **Custom**.
14. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.

    Go to step 22.
15. If you are configuring a 256-port director, select the **Configure for** *<256-Port_Director_Name>* check box.
    - If you selected **Configure for** *<256-Port_Director_Name>*, go to step 19.
    - If you did not select **Configure for** *<256-Port_Director_Name>*, continue with step 16.

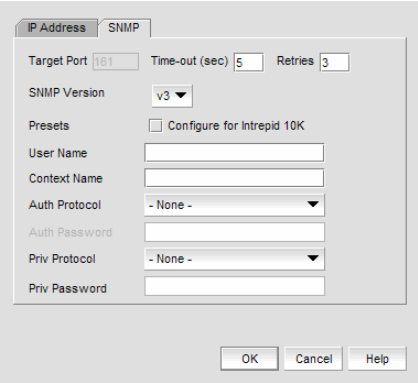


FIGURE 10 **Address Properties Dialog Box (SNMP Tab - v3)**

16. Enter a user name in the **User Name** field.
17. Enter a context name In the **Context Name** field.
18. Select the authorization protocol in the **Auth Protocol** field.
19. Enter the authorization password in the **Auth Password** field.
    - If you selected **Configure for** *<256-Port_Director_Name>*, go to step 22.
    - If you did not select **Configure for** *<256-Port_Director_Name>*, continue with step 20.
20. Select the privacy protocol in the **Priv Protocol** field.
21. Enter the privacy password in the **Priv Password** field.

22. Click **OK** on the **Address Properties** dialog box.

    If the seed switch is partitioned, the **Undiscovered Seed Switches** dialog box displays.

    a. Select the **Select** check box for each undiscovered seed switch to discover their fabrics.

    b. Click **OK** on the **Undiscovered Seed Switches** dialog box.

23. Click **OK** on the **Discover Setup** dialog box.

Configuring SNMP credentials

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.

2. Select an IP address from the **Available Addresses** table.
3. Click **Edit**.

   The **Address Properties** dialog box displays.

4. Click the **SNMP** tab.
5. Select the SNMP version from the **SNMP Version** list.
   - If you selected v1, continue with step 6.
   - If you select v3, the **SNMP** tab displays the v3 required parameters. Go to step 10.
6. Specify the **Read** option by selecting **Default 'public'** or **Custom**.
7. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.
8. Specify the **Write** option by selecting **Default 'private'** or **Custom**.
9. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.

   Go to step 22.

10. If you are configuring a 256-Port director, select the **Configure for** *<256-Port_Director_Name>* check box.
    - If you selected **Configure for** *<256-Port_Director_Name>*, go to step 14.
    - If you did not select **Configure for** *<256-Port_Director_Name>*, continue with step 11.

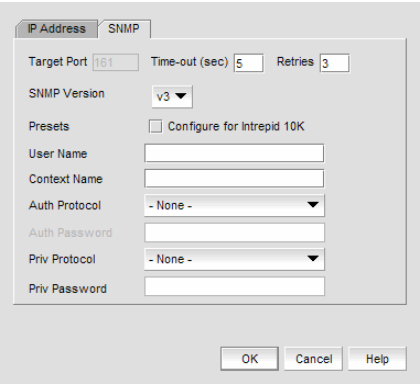


FIGURE 11 **Address Properties Dialog Box (SNMP Tab - v3)**

11. Enter a user name in the **User Name** field.

12. Enter a context name In the **Context Name** field.
13. Select the authorization protocol in the **Auth Protocol** field.
14. Enter the authorization password in the **Auth Password** field.
    - If you selected **Configure for** *<256-Port_Director_Name>*, go to step 17.
    - If you did not select **Configure for** *<256-Port_Director_Name>*, continue with step 15.
15. Select the privacy protocol in the **Priv Protocol** field.
16. Enter the privacy password in the **Priv Password** field.
17. Click **OK** on the **Address Properties** dialog box.

    If the seed switch is not partitioned, continue with step 18.

    If the seed switch is partitioned, the **Undiscovered Seed Switches** dialog box displays.

    a. Select the **Select** check box for each undiscovered seed switch to discover their fabrics.

    b. Click **OK** on the **Undiscovered Seed Switches** dialog box.
18. Click **OK** on the **Discover Setup** dialog box.

Reverting to a default SNMP community string

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.
2. Select an IP address from the **Available Addresses** table.
3. Click **Edit**.

   The **Address Properties** dialog box displays.
4. Click the **SNMP** tab.
5. Click **Default 'public'** and **Default 'private**.'
6. Click **OK** on the **Address Properties** dialog box.
7. Click **OK** on the **Discover Setup** dialog box.

Deleting a fabric

If you decide you no longer want the Management application to discover and monitor a specific fabric, you can delete it. Deleting a fabric also deletes the fabric data on the server (both system collected and user-defined data) except for user-assigned names for the device port, device node, and device enclosure information.

To delete a fabric, complete the following steps.

1. Select **Discovery** > **Setup**.

   The **Discover Setup** dialog box displays.
2. Select the fabric for which you want to delete from the **Discovered Addresses** table.
3. Click **Delete**.

   You are prompted to confirm that you want to delete the fabric.

Host discovery

The Management application enables you to discover individual hosts, import a group of Host from a CSV file, or import all hosts from discovered fabrics.

NOTE
Host discovery requires HCM Agent 2.0 or later.

NOTE
SMI and WMI discovery are not supported.

Discovering Hosts by IP address or hostname

To discover a Host by IP address or hostname, complete the following steps.

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.

2. Click **Add Host**.

   The **Add Host Discovery** dialog box displays.

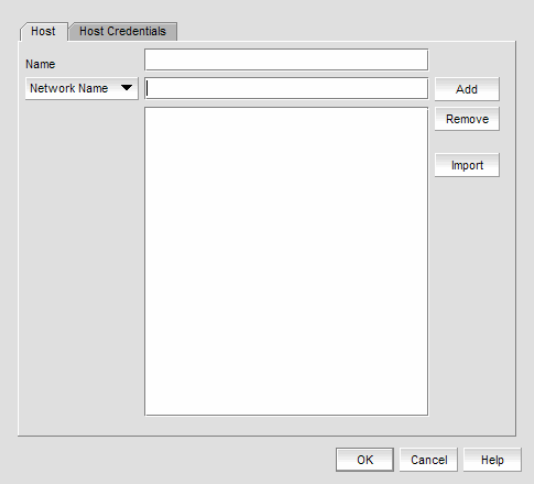


FIGURE 12 Add Host Discovery dialog box - Host tab

3. Enter a discovery request name (such as, Manual 06/12/2009) in the **Name** field.
4. Select **Network Address** from the list.
5. Enter the IP address (IPv4 or IPv6 formats) or hostname in the **Network Address** field.
6. Click **Add**.

   The IP address or hostname of the Host displays in the text box.

7. Configure Host credentials, if necessary.

   To configure host credentials, refer to "Configuring Brocade HBA credentials" on page 47 or "Configuring virtual machine credentials" on page 48.

8. Repeat step 5 through step 7 for each Host you want to discover.

9. Click **OK** on the **Add Host Discovery** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

   A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.

10. Click **Close** on the **Discover Setup** dialog box.

Importing Hosts from a CSV file

To discover Hosts by importing a CSV file, complete the following steps.

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.

2. Click **Add Host**.

   The **Add Host Discovery** dialog box displays.

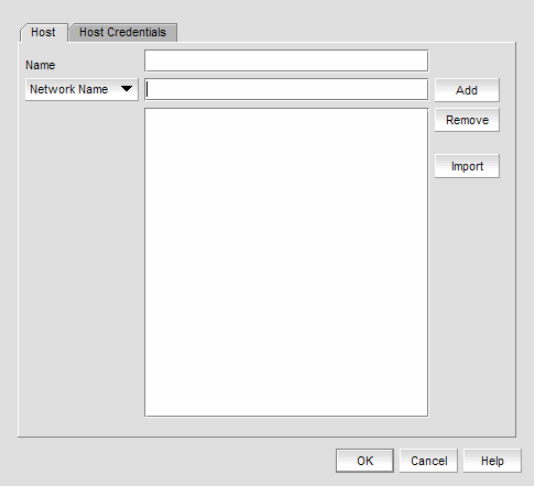


FIGURE 13 **Add Host Discovery dialog box - Host tab**

3. Click **Import**.

   The **Open** dialog box displays.

4. Browse to the CSV file location.

   The CSV file must meet the following requirements:

   - Comma separated IP address or host names
   - No commas within the values
   - No escaping supported

     For example, XX.XX.XXX.XXX, XX.XX.X.XXX, computername.company.com

5. Click **Open**.

   The CSV file is imported to the **Add Host** dialog box. During import, duplicate values are automatically dropped. When import is complete, the imported values display in the Host list text box. If the file cannot be imported, an error displays.

6. Verify the imported values in the **Host List** text box.
7. Configure Host credentials, if necessary.

   To configure host credentials, refer to "Configuring Brocade HBA credentials" on page 47 or "Configuring virtual machine credentials" on page 48.
8. Click **OK** on the **Add Host Discovery** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

   A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.
9. Click **Close** on the **Discover Setup** dialog box.

Importing Hosts from a Fabric

To discover a Host from a discovered fabric, complete the following steps.

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.
2. Click **Add Host**.

   The **Add Host Discovery** dialog box displays.

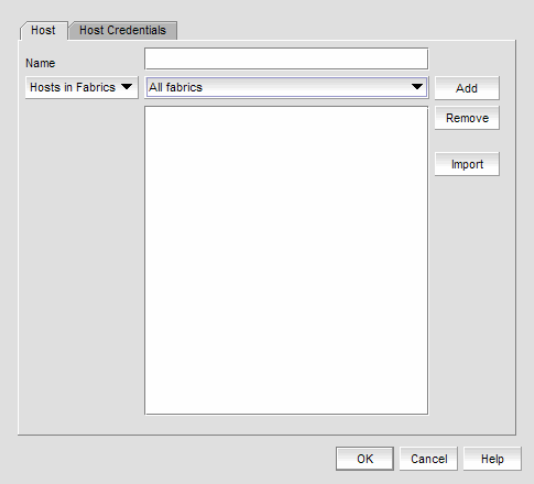


FIGURE 14 Add Host Discovery dialog box - Host tab

3. Enter a discovery request name (such as, MyFabric) in the **Name** field.
4. Select **Hosts in Fabric** from the list.
5. Select **All fabrics** or an individual fabric from the list.
6. Click **Add**.

   All hosts which are part of a managed fabric and have a registered host name display in the text box. If no host with a registered host name exists, an error message displays. Click **OK** to close the error message.

7. Configure Host credentials, if necessary.

   To configure host credentials, refer to "Configuring Brocade HBA credentials" on page 47 or "Configuring virtual machine credentials" on page 48.

8. Click **OK** on the **Add Host Discovery** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

   A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.

9. Click **Close** on the **Discover Setup** dialog box.

Configuring Brocade HBA credentials

To configure credentials for a Brocade HBA, complete the following steps.

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.

2. Click **Add Host**.

   The **Add Host Discovery** dialog box displays.

3. Discover a host.

   To discover a host, refer to "Discovering Hosts by IP address or hostname" on page 44, "Importing Hosts from a CSV file" on page 45, or "Importing Hosts from a Fabric" on page 46.

4. Click the **Host Credentials** tab.

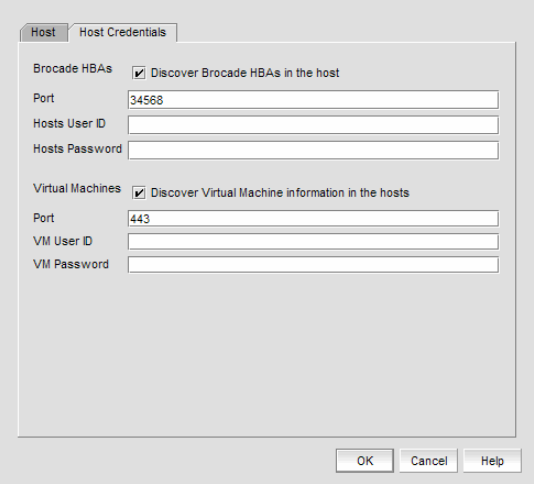


FIGURE 15 **Add Host Discovery dialog box - Host Credentials tab**

5. Select the **Discover Brocade HBAs in the hosts** check box, if necessary.
6. Enter the HCM Agent port number in the **Brocade HBAs - Port** field if necessary.
7. Enter your username and password in the appropriate fields.

8. Click **OK** on the **Add Host Discovery** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

   A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.

9. Click **Close** on the **Discover Setup** dialog box.

Configuring virtual machine credentials

To configure credentials for a virtual machine, complete the following steps.

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.

2. Click **Add Host**.

   The **Add Host Discovery** dialog box displays.

3. Discover a host.

   To discover a host, refer to "Discovering Hosts by IP address or hostname" on page 44, "Importing Hosts from a CSV file" on page 45, or "Importing Hosts from a Fabric" on page 46.

4. Click the **Host Credentials** tab.

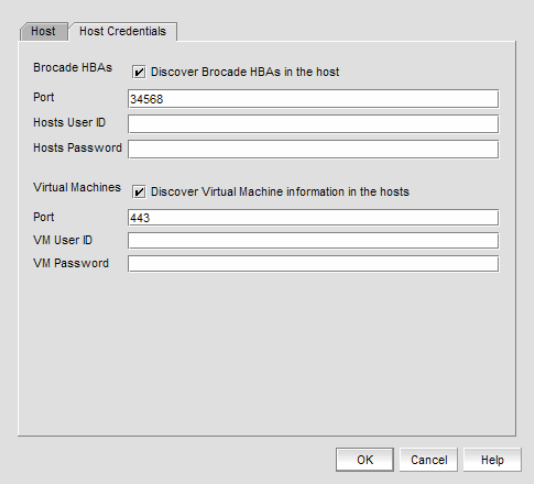


FIGURE 16 **Add Host Discovery dialog box - Host Credentials tab**

5. Select the **Discover Brocade HBAs in the hosts** check box, if necessary.
6. Enter the HCM Agent port number in the **Brocade HBAs - Port** field if necessary.
7. Enter your username and password in the appropriate fields.
8. Select the **Discover virtual machine information in the hosts** check box.
9. Enter the virtual machine port number in the **Brocade HBAs - Port** field if necessary.
10. Enter your username and password in the appropriate fields.

11. Click **OK** on the **Add Host Discovery** dialog box.

    If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

    A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.

12. Click **Close** on the **Discover Setup** dialog box.

Editing Host credentials

To edit Host credentials, complete the following steps.

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.

2. Select the Host and click **Edit**.

   The **Edit Host Discovery** dialog box displays.

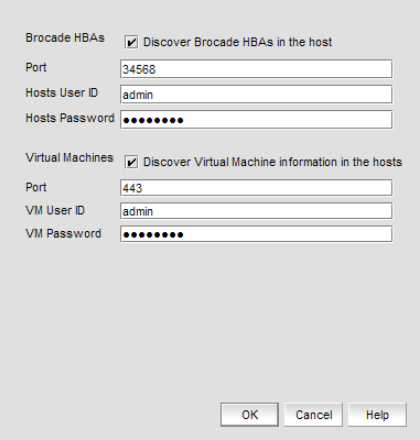


FIGURE 17 Edit Host Discovery dialog box

3. To edit Brocade HBA credentials, select the **Discover Brocade HBAs in the hosts** check box, if necessary, and complete the following steps.

   a. Enter the HCM Agent port number in the **Brocade HBAs - Port** field if necessary.

   b. Enter your username and password in the appropriate fields.

4. To edit virtual machine credentials, select the **Discover virtual machine information in the hosts** check box, if necessary, and complete the following steps.

   a. Enter the virtual machine port number in the **Brocade HBAs - Port** field if necessary.

   b. Enter your username and password in the appropriate fields.

5. Click **OK** on the **Edit Host Discovery** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

6. Click **Close** on the **Discover Setup** dialog box.

Removing a Host from Discovery

To remove a Host from discovery, complete the following steps.

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.

2. Select the Host you want to remove from discovery.
3. Click **Delete**.
4. Click **OK** on the confirmation message.

   The deleted host displays in the **Previously Discovered Addresses** table.

5. Click **Close** on the **Discover Setup** dialog box.

Viewing the discovery state

The Management application enables you to view device status through the **Discover Setup** dialog box.

To view the discovery status of a device, complete the following steps.

1. Select **Discover > Setup**.

   The **Discover Setup** dialog box displays.

2. Right-click a fabric and select **Expand All** to show all devices in the fabric.

   The **Name** field displays the discovery status icons in front of the device name. The following table illustrates and describes the icons that indicate the current status of the discovered devices.

TABLE 12 Discovery Status Icons

Icon	Description
	Displays when the fabric or host is managed and the management status is okay.
	Displays when the fabric is managed and the switch management status is not okay.
	Displays when the fabric or host is not managed.

The **Discovery Status** field details the actual status message text, which varies depending on the situation. The following are samples of actual status messages:

- Discovered: Seed Switch: Not registered for SNMP Traps
- Discovered: Seed Switch: Not Manageable: Not registered for SNMP Traps
- Discovered: Current seed switch is not recommended. Change Seed Switch. : Seed Switch: Not registered for SNMP Traps
- New Discovery Pending

- Created host structure differs from discovered host; Discovery ignored
- Brocade HBA Discovery Failed: HCM Agent connection failed

Troubleshooting discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly.

1. Verify IP connectivity by issuing a ping command to the switch.
   a. Open the command prompt.
   b. From the Server, type `ping <switch IP address>`.
2. Enter the IP address of the device in a browser to verify the SNMP settings.

   For example, *http://10.1.1.11*.

Fabric monitoring

NOTE
Monitoring is not supported on Hosts.

Fabric monitoring enables discovery of and data collection for the specified fabric and all associated devices. The Management application enables you to view fabric monitoring status through the **Discover Setup** dialog box. The following table illustrates and describes the icons that indicate the current status of the discovered fabrics.

TABLE 13 Monitor Icons

Icon	Description
	Displays when the fabric is managed and the switch management status is okay.
	Displays when the fabric is managed and the switch management status is not okay.
	Displays when the fabric is not managed.

Monitoring discovered fabrics

NOTE
Monitoring is not supported on Hosts.

To monitor a fabric and all associated devices, complete the following steps.

1. Select **Discovery** > **Setup**.

   The **Discover Setup** dialog box displays.

2. Select the fabric you want to monitor from the **Discovered Addresses** table.
3. Click **Monitor**.

   The monitor function fails if the fabric has user-defined Admin Domains created or if the fabric is merged with another fabric already in the monitored state.

4. Click **OK**.

Stop monitoring of a discovered fabric

NOTE
Monitoring is not supported on Hosts.

When you stop monitoring of a fabric, you stop discovery of and data collection for the specified fabric and all associated devices.

To stop monitoring a fabric and all associated devices, complete the following steps.

1. Select **Discovery** > **Setup**.

   The **Discover Setup** dialog box displays.

2. Select the fabric you want to stop monitoring from the **Discovered Addresses** table.
3. Click **Unmonitor**.
4. Click **OK**.

Seed switch

The seed switch must be running a supported Fabric OS version and must be HTTP-reachable.

Sometimes, the seed switch is auto-selected, such as when a fabric segments or when two fabrics merge. Other times, you are prompted (an event is triggered) to change the seed switch, such as in the following cases:

- If, during fabric discovery, the Management application detects that the seed switch is not running a supported version, you are prompted to change the seed switch.
- When one or more switches join the fabric or if the switch firmware is changed on any of the switches in the fabric, the Management application checks to make sure that the seed switch is still running a supported version. If it is not, then you are prompted to either upgrade the firmware on the seed switch or to change the seed switch to a switch running a supported firmware.

If a fabric of switches running only Fabric OS 5.X or later is created due to segmentation, the Management application continues to monitor that fabric, but if any switch with a later Fabric OS version joins the fabric, an event is triggered informing you that the seed switch is not running the latest firmware and you should change to the seed switch running the highest firmware.

ATTENTION
If a seed switch is segmented or merged, historical data such as offline zone DB, profile and reports, and Firmware Download Profile can be lost. Segmentation of a seed switch does not result in formation of a new fabric. If a merge occurs, the historical data is lost only from the second fabric.

You can change the seed switch as long as the following conditions are met:

- The new seed switch is HTTP-reachable from the Management application.
- The new seed switch is a primary FCS.
- The new seed switch is running the latest Fabric OS version in the fabric.

This operation preserves historical and configuration data, such as performance monitoring and user-customized data for the selected fabric.

ATTENTION
If the seed switch firmware is downgraded from Fabric OS 5.2.X to an earlier version, then all RBAC-related data is discarded from the Management application.

If, during the seed switch change, the fabric is deleted, but the rediscovery operation fails (for example, if the new seed switch becomes unreachable using HTTP), then you must rediscover the fabric again. If you rediscover the fabric using a switch that was present in the fabric before the change seed switch operation was performed, then all of the historical and configuration data is restored to the rediscovered fabric. If you rediscover the fabric using a switch that was added to the fabric after the fabric was deleted, then the historical and configuration data is lost.

If multiple users try to change the seed switch of the same fabric simultaneously, only the first change seed switch request is executed; subsequent requests that are initiated before the first request completes will fail.

If another user changes the seed switch of a fabric you are monitoring, and if you have provided login credentials for only that seed switch in the fabric, then you lose connection to the seed switch.

Seed switch requirements

Depending on your environment, you must meet the following hardware and firmware version requirements for seed switches.

Fabric OS devices:

- For Fabric OS only fabrics, the seed switch must be running Fabric OS 5.0 or later.
- For mixed fabrics (Fabric OS and M-EOS), the seed switch must be running Fabric OS 6.0 or later.

  For a complete list of all supported Fabric OS hardware, refer to "Supported hardware and software" on page xx.

Seed switch failover

The Management application collects fabric-wide data (such as, fabric membership, connectivity, name server information, zoning, and so on) using the seed switch. Therefore when a seed switch becomes unreachable or there is no valid seed switch, the fabric becomes unmanageable.

When the seed switch cannot be reached for three consecutive fabric refresh cycles, the Management application looks for another valid seed switch in the fabric, verifies that it can be reached, and has valid credentials. If the seed switch meets this criteria, the Management application automatically fails over to the recommended seed switch.

Note that it is possible that auto-failover may occur to a seed switch not running the latest firmware version. In this instance, any functionality which has a direct dependency on the firmware version of the seed switch is affected and restricted by the failover seed switch capabilities.

Changing the seed switch

When you change the seed switch for a fabric, the Management application performs the following checks in the order they are listed:

- Identifies all switches and removes those running unsupported firmware version.
- Identifies which of the remaining switches are running the latest firmware versions.
- Filters out those switches that are not reachable.
- Identifies which switches are Virtual Fabric-enabled switches (Fabric OS only).

  If there are Virtual Fabric-enabled switches, the Management application only uses these switches as recommended seed switches. If there are no Virtual Fabric-enabled switches, continue with the next check.
- Identifies which switches are Virtual Fabric-capable devices (Fabric OS only).

  If there are Virtual Fabric-capable switches, the Management application only uses these switches as recommended seed switches. If there are no Virtual Fabric-capable switches, the Management application uses the list from the second check.

To change the seed switch, complete the following steps.

1. Select **Discovery** > **Setup**.

   The **Discover Setup** dialog box displays.

2. Select the fabric for which you want to change the seed switch from the **Discovered Addresses** table.

   If a device joins or merges with a fabric and fabric tracking is active, you must accept changes to the fabric before the new devices display in the **Change Seed Switch** dialog box. For more information about fabric tracking, refer to "Fabric tracking" on page 110.

3. Click **Change Seed Switch**.

   If the fabric contains other switches that are running the latest version and are also HTTP-reachable from the Management application, the **Change Seed Switch** dialog box appears. Otherwise, a message displays that you cannot change the seed switch.

4. Select a switch to be the new seed switch from the **Change Seed Switch** dialog box.

   You can select only one switch. Only switches that are running the latest Fabric OS version in the fabric are displayed. The current seed switch is not displayed in this list.

5. Click **OK**.

   If you are not already logged in to the seed switch, the **Fabric Login** dialog box displays.

   If you are successfully authenticated, the fabric is deleted from the Management application without purging historical data, and the same fabric is rediscovered with the new seed switch.

6. Click **OK**.

Chapter

3

Application Configuration

In this chapter

- Management server and client 58
- Data backup 70
- Data restore 77
- Display 79
- End node display 80
- Ethernet events 81
- Event storage 82
- Flyovers 83
- Names 87
- Security 93
- Software Configuration 96
- Topology layout 115

Management server and client

The Management application has two parts: the Server and the Client. The Server is installed on one machine and stores SAN-related information; it does not have a user interface. To view SAN information through a user interface, you must log in to the Server through a Client. If you are running Professional Edition, the server and the client must be on the same machine.

In some cases, a network may utilize virtual private network (VPN) or firewall technology, which can prohibit communication between Switches and the Servers or Clients. In other words, a Server or Client can find a Switch, appear to log in, but is immediately logged out because the Switch cannot reach the Server or Client. To resolve this issue, check to determine if the ports in the table below need to be opened up in the firewall.

NOTE
Professional Edition does not support remote clients.

TABLE 14 Ports

Port Number	Ports	Description	Communication Path	Open in Firewall
20[1]	FTP Port (Control)	FTP Control port for internal FTP server	Client–Server Switch–Server	No Yes
21[1, 2]	FTP Port (Data)	FTP Data port for internal FTP server	Client–Server Switch–Server	No Yes
22[1]	SSH or Secure Telnet	Sectelnet port from server to switch/client to switch	Server–Switch Client–Switch	Yes
23[1]	Telnet	Telnet port from server/client to switch	Server–Switch Client–Switch	Yes
25	SMTP Server port	SMTP Server port for E-mail communication	Server–SMTP Server	Yes
80	jboss.web.http.port	Non-SSL HTTP/1.1 connector port	Client–Server	No
80[3, 4, 5]	Switch http	Switch non-SSL http port for http and CAL communication	Server–Switch Client–Switch	Yes
161[1]	SNMP Port	Default SNMP port	Server–Switch	Yes
162[3]	snmp.trap.port	Default SNMP trap port	Switch–Server	Yes
514[6]	Syslog Port	Default Syslog Port	Switch–Server	Yes
1527	Database port (Enforced during install)	Port used by database	Server–Database Remote ODBC–Database	No
24600	jboss.naming.jnp.port - port 0	Bootstrap JNP service port	Client–Server	No
24601	jboss.connector.ejb3.port - port 1	EJB3 connector port	Client–Server	No
24602	jboss.connector.bisocket.port - port 2	Bisocket connector port	Client–Server	No
24603	jboss.connector.bisocket.secondary.port - port 3	Bisocket connector secondary port	Client–Server	No
2460[6]	jboss.naming.rmi.port - port 4	RMI naming service port	Client–Server	No

TABLE 14 Ports

Port Number	Ports	Description	Communication Path	Open in Firewall
246	jboss.jrmp.invoker.port - port 5	RMI/JRMP invoker port	Client–Server	No
246[7]	jboss.pooled.invoker.port - port 6	Pooled invoker port	Client–Server	No
246	jboss.connector.socket.port - port 7	Socket invoker port	Server	No
2461[3]	jboss.web.ajp.port - port 8	AJP 1.3 connector port	Server	No
2461[1]	jboss.web.service.port – port 9	Web service port	Server	No
2461[2]	connector.bind.port – port 10	Port to listen for requests on	Server	No

1 Port is not configurable (either in the switch or the Management server).

2 Every FTP session requires an additional port which is randomly picked. If the firewall is enabled then FTP operation (used for firmware download, technical support, firmware import (from client-server) and so on.) will fail.

3 Ports configurable in the switch and the Management server. Port must be the same for all switches managed by the Management server.

4 Ports used to launch the Web Tools application for Fabric OS switches from the Management client. This is applicable only when the FOS version is earlier than 6.1.1.

5 Port 80 is the default web server port number. If you set the web server port number to a port other than the default, you must open that port in the firewall.

6 The Syslog listening port is configurable in the Management server. The switch always sends syslog messages to port 514. If you have any other syslog daemon on the Management server machine already listening to 514, then the Management Server can be configured to listen to a different port. You must manually configure relay in existing syslogd to forward the syslog messages to the Management Server listening on the configured port.

7 The Management server tries to find a contiguous block of 13 ports from the starting port configured (for example, 24600); if any port in this range is not available for the Management application, then you must provide a new starting port. Note that Port 1 to Port 12 in “Ports” column of the table above are not separately configurable and those ports vary based on the starting port number configuration (specified as Port 0 in the above table). The port numbers mentioned in the table above are the default ports (for example, when 24600 is selected as the starting port number).

Logging into a server

You must log into a Server to monitor a SAN.

NOTE
You must have an established user account on the Server to log in.

To log into a server, complete the following steps.

1. Double-click the desktop icon or open the application from the **Start** menu.

   The **Log In** dialog box displays (Figure 18).

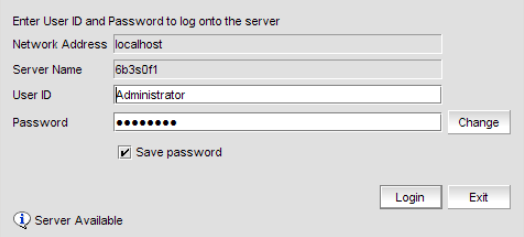


FIGURE 18 Log In Dialog Box

2. Enter your user name and password.

   The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

3. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.

4. Click **Login**.

5. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Logging into a remote client

To log into a remote client, complete the following steps.

1. Open a web browser and enter the IP address of the Management application server in the **Address** bar.

   If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *<IP_Address>:<Web_Server_Port_Number>*.

   The Management application web start screen displays.

2. Click the Management application web start link.

   The **Log In** dialog box displays (Figure 19).

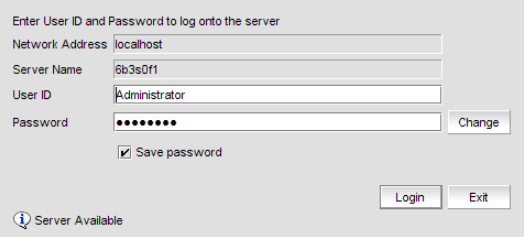


FIGURE 19 Log In Dialog Box

3. Enter your user name and password.

   The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

4. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.

5. Click **Login**.

6. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Changing your password

To change your password, complete the following steps.

1. Double-click the desktop icon or open from the **Start** menu.

   The **Log In** dialog box displays.

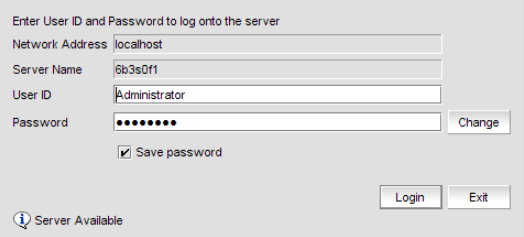


FIGURE 20 **Log In Dialog Box**

2. Enter your user name and password.

   The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

3. Click **Change**.

   The **Change Password** dialog box displays.

4. Enter your new password in the **Secure Password** and **Retype Password** fields and click **OK**.
5. Click **Login**.
6. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Changing the database user password

To change the database password, complete the following steps in the <Install_Home>/bin directory.

1. Open a command window.
2. Type **dbpassword** *<User_Name> <Password> <New_Password> <Confirm_Password>* and press **Enter**.

   Where *<User_Name>* is your user name, *<Password>* is your current password, and *<New_Password>* and *<Confirm_Password>* are your new password. The user name and password defaults are dcfm and passw0rd (zero), respectively.

   If the password changed successfully, the following message displays:
   Password changed successfully.

   If an error occurs and the password did not change, the following message displays:
   Error while updating password. Please try again.
   Press any key to continue.

   If the current password and new password are the same, the following message displays:
   Old and New passwords cannot be same. Use different password and try again.
   Press any key to continue.

   If the new password and confirm password do not match, the following message displays:
   New password and confirm password do not match. Please try again.
   Press any key to continue.

Viewing active sessions

To view the Management application active sessions, complete the following steps.

1. Select **SAN > Active Sessions**.

   The **Active Sessions** dialog box displays (Figure 22).

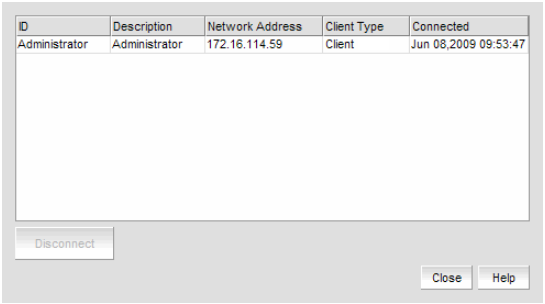


FIGURE 21 **Active Sessions dialog box**

2. Review the active session information.

   The following information displays:

   - **ID**—Displays the name of the user (for example, Administrator).
   - **Description**—Displays the description of the user (for example, Operator).
   - **Network Address**—Displays the network address of the user.

- **Client Type**—Displays the type of Management application client.
- **Connected**—Displays the date and time the user connected to the server.

3. Click **Close**.

Disconnecting users

To disconnect a user, complete the following steps.

1. Select **SAN > Active Sessions**.

   The **Active Sessions** dialog box displays.

2. Select the user you want to disconnect and click **Disconnect**.
3. Click **Yes** on the confirmation message.
4. The user you disconnected receives a 'you have been disconnected' message.
5. Click **Close**.

Viewing server properties

To view the Management application server properties, complete the following steps.

1. Select **SAN > Server Properties**.

   The **Server Properties** dialog box displays (Figure 22).

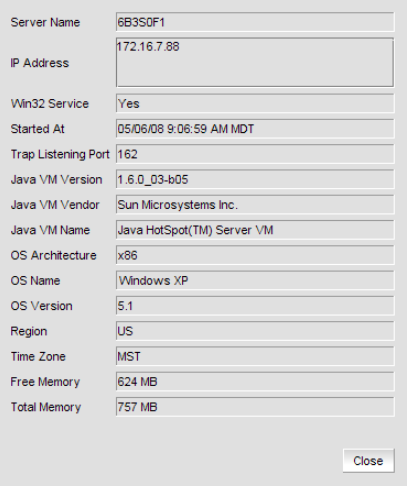


FIGURE 22 Server Properties dialog box

2. Click **Close**.

Customizing the main window

You can customize the main window to display only the data you need by displaying different levels of detail on the Connectivity Map (topology) or Product List.

Zooming in and out of the connectivity map

You can zoom in or out of the Connectivity Map to see products and ports.

Zooming In

To zoom in on the Connectivity Map, use one of the following methods:

- Click the zoom-in icon ( ) on the toolbox.
- Press CTRL + NumPad+ on the keyboard.
- Use the **Zoom** dialog box.
  a. Select **View > Zoom**.

     The **Zoom** dialog box displays (Figure 23).

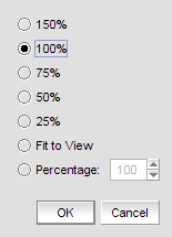


FIGURE 23 **Zoom Dialog Box**

  b. Select a zoom percentage.
  c. Click **OK** to save your changes and close the **Zoom** dialog box.

Zooming out

To zoom out of the Connectivity Map, use one of the following methods:

- Click the zoom-out icon ( ) on the toolbox.
- Press CTRL + NumPad- on the keyboard.
- Use the **Zoom** dialog box.
  a. Select **View > Zoom**.

     The **Zoom** dialog box displays.
  b. Select a zoom percentage.
  c. Click **OK** to save your changes and close the **Zoom** dialog box.

Showing levels of detail on the connectivity map

You can configure different levels of detail on the Connectivity Map, making Management easier.

View Fabrics
To view only fabrics, without seeing groups, products or ports:

Select **View > Show> Fabrics Only**.

View Groups
To view only groups and fabrics, without seeing products or ports:

Select **View > Show> Groups Only**.

View Products
To view products, groups, and fabrics:

Select **View > Show> All Products**.

View Ports
To view all ports:

Select **View > Show> All Ports**.

Customizing the application

You can customize any table in the Management application (for example, the Master Log or the Product List) in the following ways:

- Display only specific columns
- Display columns in a specific order
- Resize the columns to fit the contents
- Sort the table by a specific column or multiple columns
- Copy information from the table to another application
- Export information from the table
- Search for information
- Expand the table to view all information
- Collapse the table

Displaying columns

To only display specific columns, complete the following steps.

1. Right-click anywhere in the table and select **Customize** or **Table > Customize**.

   The **Customize Columns** dialog box displays.

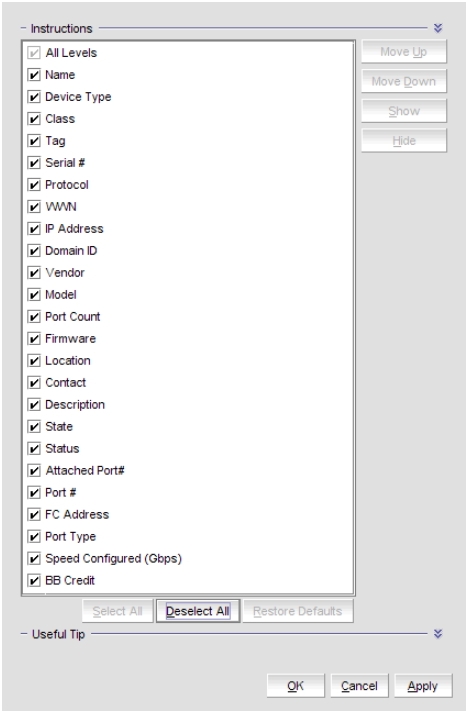


FIGURE 24 Customize Columns dialog box

2. Choose from the following options:

   - Select the check box to display a column.
     OR
     Select the column name and click **Show**.
   - Clear the check box to hide a column.
     OR
     Select the column name and click **Hide**.
   - Click **Select All** to select all check boxes.
   - Click **Deselect All** to clear all check boxes.
   - Click **Restore Defaults** to restore the Product List to the original settings.

3. Click **OK**.

Changing the order of columns

To change the order in which columns display, choose from one of the following options.

Rearrange columns in a table by dragging and dropping the column to a new location.

OR

1. Right-click anywhere in the table and select **Customize** or **Table > Customize**.

   The **Customize Columns** dialog box displays.

2. Highlight the name of the column you want to move and use **Move Up** and **Move Down** to move it to a new location.
3. Click **OK**.

Resizing the columns

You can resize a single column or all columns in the table.

To resize a single column, right-click the column header and select **Size Column to Fit** or **Table > Size Column to Fit**.

To resize all columns in the table, right-click anywhere in the table and select **Size All Columns to Fit** or **Table > Size All Columns to Fit**.

Sorting table information

To sort the product list by a single column, click the column header.

To reverse the sort order, click the column header again.

To sort the product list by multiple columns, complete the following steps.

1. Click the primary column header.
2. Press CTRL and click a secondary column header.

Copying table information

You can copy the entire table or a specific row to another application (such as, Notepad, Excel, Word, and so on).

1. Choose from one of the following options:
   - Right-click anywhere in the table and select **Table > Copy Table**.
   - Select the table row that you want to export and select **Table > Copy Row.**
2. Open the application to which you want to copy the Product List information.
3. Select **Edit > Paste** or **CTRL + V**.
4. Save the file.

Exporting table information

You can export the entire table or a specific row to a text file.

1. Choose from one of the following options:
   - Right-click anywhere in the table and select **Table > Export Table**.
   - Select the table row that you want to export and select **Table > Export Row.**

   The **Save table to a tab delimited file** dialog box displays.
2. Browse to the location where you want to save the file.
3. Enter file name in the **File Name** field.
4. Click **Save**.

Searching for information in a table

You can search for information in the table by any of the values found in the table.

1. Right-click anywhere in the table and select **Table > Search**.

   The **Search for** field displays.

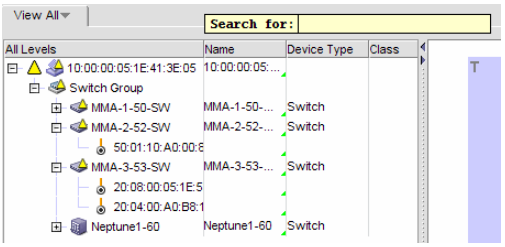


FIGURE 25 Search for field

2. Enter all or part of the search text in the **Search for** field.

   The first instance is highlighted in the table.
3. Press **Enter** to go to the next instance of the search text.

Expanding and collapsing tables

You can expand a table to display all information or collapse it to show only the top level.

To expand the entire table, right-click anywhere in the table and select **Expand All** or **Table > Expand All**.

To collapse the entire table, right-click anywhere in the table and select **Collapse All** or **Table > Collapse All**.

Searching for a device in the connectivity map

You can search for a device in the Connectivity map by name, WWN, or device type.

1. Enter all or part of the device type, name, or WWN in the search field.
2. Press **Enter** or click **Search**

Data backup

The Management application helps you to protect your data by backing it up automatically. The data can then be restored, as necessary.

NOTE
Backing up data takes some time. It is possible that, in a disaster recovery situation, configuration changes made after the last backup interval will be missing from the backup.

The Management application allows you to view the backup status at a glance, initiate immediate backup, enable or disable automatic backup, reconfigure the backup directory, interval, and start time, and retrieve backup events.

What is backed up?

The data is backed up to the following directories:

- Backup\databases — contains database and log files.
- Backup\data — contains M-EOS switches Element Manager data files (including Dump files, Data collection progress files, Director/Switch firmware files FAF files, Switch technical supportSave, and Switch backup files) and Fabric OS miscellaneous files.
- Backup\conf – contains the Management application configuration files.

Management server backup

There are three options for backing up data to the management server:

- Configuring backup to a writable CD
- Configuring backup to a hard drive
- Configuring backup to a network drive

The Management Server is backed up to a rewritable (CD-RW) compact disk by default. Make sure you have a CD-RW disk in the CD recorder drive to ensure that backup can occur. Critical information from the Management application is automatically backed up to the CD-RW when the data directory contents change or when you restart the Management application.

Note that backing up to CD is not the recommended method. The usable capacity of a CD is approximately 700 MB and needs to be replaced when full. Also, CD media has a limited number of re-writes before the medium is exhausted, and write errors occur. It is recommended that you configure the backup system to target a hard drive or a network drive as described in the procedures below.

Back up directory structure overview

The Management server backs up data to two alternate folders. For example, if the backup directory location is D:\Backup, the backup service alternates between two backup directories, D:\Backup and D:\BackupAlt. The current backup is always D:\Backup and contains a complete backup of the system. The older backup is always D:\BackupAlt.

If a backup cycle fails, the cause is usually a full CD-RW. When the backup cycle fails, there may only be one directory, D:\Backup. There may also be a D:\BackupTemp directory. Ignore this directory because it may be incomplete.

Configuring backup to a writable CD

NOTE
This is not recommended on a permanent basis. CDs have a limited life, and may only last a month. An error message occurs if your Management application can no longer back up to the disc.

To configure the backup function to a writable CD, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 26).

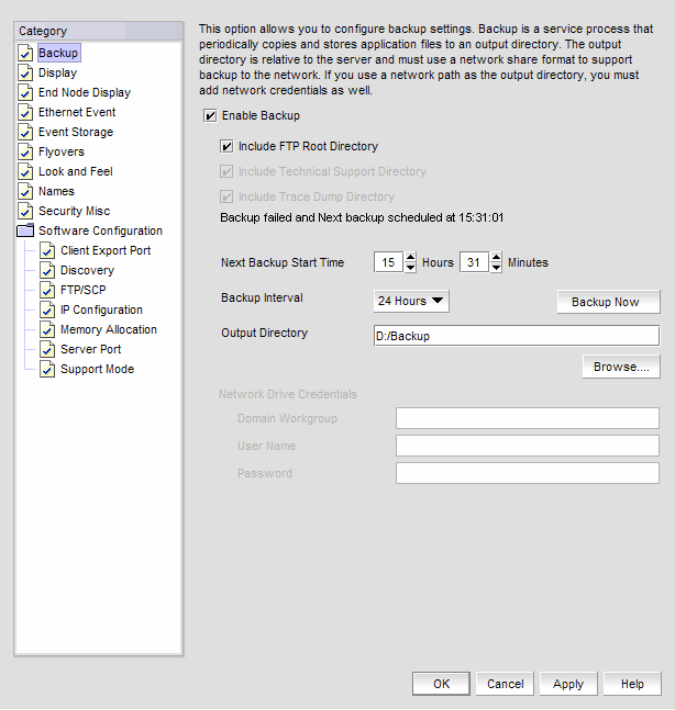


FIGURE 26 **Options Dialog Box (Backup option)**

2. Select **Backup** in the **Category** list.

   The currently defined directory displays in the **Backup Output Directory** field.

3. Select the **Enable Backup** check box, if necessary.

4. Choose one or more of the following options:
   - Select the **Include FTP Root Directory** check box.

     If you select the FTP Root directory, the FTP Root sub-directories, Technical Support and Trace Dump, are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.
   - Select the **Include Technical Support Directory** check box, if necessary.
   - Select the **Include Trace Dump Directory** check box, if necessary.
5. Enter the time (using a 24-hour clock) you want the backup process to begin in the **Next Backup Start Time Hours** and **Minutes** fields.
6. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
7. Verify that the CD backup directory is correct (default directory is D:\Backup).

   It is assumed that drive D is a CD-RW drive.

   You can change the directory or use the **Browse** button to select another directory.
8. Install the formatted disc into the CD drive.

   To back up to a writable CD, you must have CD-writing software installed. The disc must be formatted by the CD-writing software so that it behaves like a drive.
9. Click **Apply** or **OK**.

   The application verifies that the backup device exists and that the server can write to it. If the device does not exist or is not writable, an error message displays that says you have entered an invalid device. Click **OK** to go back to the **Options** dialog box and fix the error.

   Backup occurs, if needed, at the interval you specified.

Configuring backup to a hard drive

NOTE
This requires a hard drive. The drive should not be the same physical drive on which your Operating System or the Management application is installed.

To configure the backup function to a hard drive, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.
2. Select **Backup** in the **Category** list.

   The currently defined directory displays in the **Backup Output Directory** field.
3. Select the **Enable Backup** check box, if necessary.

4. Choose one or more of the following options:
   - Select the **Include FTP Root Directory** check box.

     If you select the FTP Root directory, the FTP Root sub-directories, Technical Support and Trace Dump, are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.
   - Select the **Include Technical Support Directory** check box, if necessary.
   - Select the **Include Trace Dump Directory** check box, if necessary.
5. Enter the time (using a 24-hour clock) you want the backup process to begin in the **Next Backup Start Time Hours** and **Minutes** fields.
6. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
7. Browse to the hard drive and directory to which you want to back up your data.
8. Click **Apply** or **OK**.

   The application verifies that the backup device exists and that the server can write to it.

   If the device does not exist or is not writable, an error message displays that states you have entered an invalid device. Click **OK** to go back to the Options dialog box and fix the error.

   Backup occurs, if needed, at the interval you specified.

Configuring backup to a network drive

To back up to a network drive, your workstation can be either in the same domain or in the same workgroup. However, you must have rights to copy files for the network drive.

NOTE
The Management application should not directly access local or network resources through mapped drive letters. When the Management application must access a remote resource (or any process that is running in a different security context), you should use the Universal Naming Convention (UNC) name to access the resource. For more information about services and redirected drives, refer to http://support.microsoft.com/kb/180362/en-us.

NOTE
Configuring backup to a network drive is not supported on UNIX systems.

NOTE
It is recommended that this configuration be completed on the Local client (the client application running on the Server) so that the backup path and location can be confirmed.

To configure the backup function to a network drive, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.
2. Select **Backup** in the **Category** list.

   The currently defined directory displays in the **Backup Output Directory** field.
3. Select the **Enable Backup** check box, if necessary.

4. Choose one or more of the following options:
   - Select the **Include FTP Root Directory** check box.

     If you select the FTP Root directory, the FTP Root sub-directories, Technical Support and Trace Dump, are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.
   - Select the **Include Technical Support Directory** check box, if necessary.
   - Select the **Include Trace Dump Directory** check box, if necessary.
5. Enter the time (using a 24-hour clock) you want the backup process to begin in the **Next Backup Start Time Hours** and **Minutes** fields.
6. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
7. Click **Browse** to choose the network share and directory to which you want to back up your data, or enter the network share and directory path.

   NOTE
   You must specify the directory in a network share format (for example, \\network-name\share-name\directory). Do not use the drive letter format (C:\directory).

8. If you want to configure backup to a network drive on a Windows system, complete the following steps.
   a. Enter the name of the Windows domain or workgroup in which you are defined in the **Domain Workgroup** field.

      NOTE
      You must be authorized to write to the network device.

   b. Enter your Windows login name in the **User Name** field.
   c. Enter your Windows password in the **Password** field.
9. Click **Apply** or **OK**.

   The application verifies that the device is accessible and that the server can write to it.

   If the device does not exist or you are not authorized to write to the network drive, an error message displays that states you have entered an invalid device path or invalid network credentials. Click **OK** to go back to the Options dialog box and fix the error.

   Backup occurs, if needed, at the interval you specified.

Enabling backup

Backup is enabled by default. However, if it has been disabled, complete the following steps to enable the function.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Backup** in the **Category** list.
3. Select the **Enable Backup** check box.
4. Click **Apply** or **OK**.

Disabling backup

Backup is enabled by default. If you want to stop the backup process, you need to disable backup. To disable the backup function, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Backup** in the **Category** list.
3. Clear the **Enable Backup** check box.
4. Click **Apply** or **OK**.

Viewing the backup status

The Management application enables you to view the backup status at a glance by providing a backup status icon on the Status Bar. The following table illustrates and describes the icons that indicate the current status of the backup function.

TABLE 15 Backup Icons

Icon	Description
	Backup in Progress—displays the following tooltip: “Backup started at hh:mm:ss, in progress... *XX* directories are backed up.”
	Countdown to Next Scheduled Backup—displays the following tooltip: “Next backup scheduled at hh:mm:ss.”
	Backup Disabled—displays the following tooltip: “Backup is disabled.”
	Backup Failed—displays the following tooltip: “Backup failed at hh:mm:ss mm/dd/yyyy.”

Changing the backup interval

When the backup feature is enabled, your SAN is protected by automatic backups. The backups occur every 24 hours by default. However, you can change the interval at which backup occurs.

ATTENTION
Do NOT modify the backup.properties file.

To change the backup interval, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Backup** in the **Category** list.
3. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
4. Click **Apply** or **OK**.

   The minimum value is 6 hours and the maximum value is 24 hours.

Starting immediate backup

NOTE
You must have backup privileges to use the Backup Now function.

To start the backup process immediately, complete one of the following procedures:

Using the Backup Icon, right-click the **Backup** icon and select **Backup Now**.

OR

1. Using the **SAN** menu, select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Backup** in the **Category** list.
3. Click **Backup Now**.

   The backup process begins immediately. There is no confirmation message.

4. Click **Apply** or **OK**.

Reviewing backup events

The Master Log, which displays in the lower left area of the main window, lists the events that occur on the Fabric.

If you do not see the Master Log, select **View > All Panels**.

The following backup events appear in the Master Log:

- Backup started
- Backup error
- Backup Enabled
- Backup Disabled
- Backup Now
- Backup destination change
- Backup interval change
- Backup start time change
- Domain workgroup change
- User name change
- User password change
- Number of files backed up on completion
- Network share access problem when backup starts or during backup (not when the backup configuration is changed)

Data restore

NOTE
You cannot restore data from a previous version of the Management application.

NOTE
You cannot restore data from a different edition of the Management application.

The Management application helps you to protect your data by backing it up automatically. The data can then be restored, as necessary.

The data in the following directories is automatically backed up to disk. The data includes the following items:

- Backup\databases — contains database and log files.
- Backup\data — contains M-EOS switches Element Manager data files (including Dump files, Data collection progress files, Director/Switch firmware files FAF files, Switch technical supportSave, and Switch backup files) and Fabric OS miscellaneous files.
- Backup\conf – contains the Management application configuration files.

In a disaster recovery situation, it is possible that configuration changes made less than 45 minutes before Server loss (depending on the backup interval you set) could be missing from the backup.

Restoring data

1. (Windows) Open the **Server Management Console** from the **Start** menu on the Management application server.

   OR

   (UNIX) Open <*Install_Home*>*/bin* from the Management application server and type `./smc.sh` at the command line.

2. Click the **Services** tab.

   The tab lists the Management application services.

3. Click **Stop Services** to stop all of the services.
4. Click the **Restore** tab.
5. Browse to the backup location.

   Browse to the location specified in the **Output Directory** field on the **Options** dialog box - Backup pane.

6. Click **Restore**.

   Upon completion, a window displays the status of the restore operation.

7. Click the **Services** tab.

   The tab lists the Management application services.

8. Click **Start Services** to start all of the services.
9. Click **OK** to close the dialog box.

Restoring data to a new server

If your Management application server fails and you must recover information to a new server, complete the following steps.

1. Restore the data (Refer to "Restoring data" on page 78 for complete instructions).
2. Configure an explicit server IP address (Refer to "Configuring an explicit server IP address" on page 103 for complete instructions).

Display

You can reset the display to the default settings.

Resetting your display

You can reset your system to display the default display settings. Note that returning to current settings after a reset may require configuring each global fabric or group setting individually. The following table (Table 16) details the settings that change with reset and the associated default state.

TABLE 16 Display Settings

Settings	Default State
Show port	Disabled.
Show connected end device	Set to Hide All.
Map Layout	Set to default for Groups.
Line Types	Set to default for Groups.
Port Display	Set to Attached Ports only.
Map Flyovers	Set to include the following properties: • Product Display—Name, Device Type, WWN, IP Address, and Domain ID. • Connection Display—Name (port), Address, Node WWN, Port WWN, and Port #.
Product List	Set to only display basic property list.
Table Column Order	Set to default for open system.

To reset the Management application to the default display and view settings, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Display** in the **Category** list.
3. Click **Reset Display**.
4. Click **Yes** on the reset confirmation message.

   The display and view settings are immediately reset to the default display settings (as detailed in the Display Settings table).

5. Click **Apply** or **OK** to save your work.

End node display

The connectivity map can be configured to display or not display end nodes. This option enables you to set the end node display for all newly discovered fabrics. Note that disabling end node display limits the connectivity map to emphasize switch members only.

Displaying end nodes

To display end nodes when discovering a new fabric, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 27).

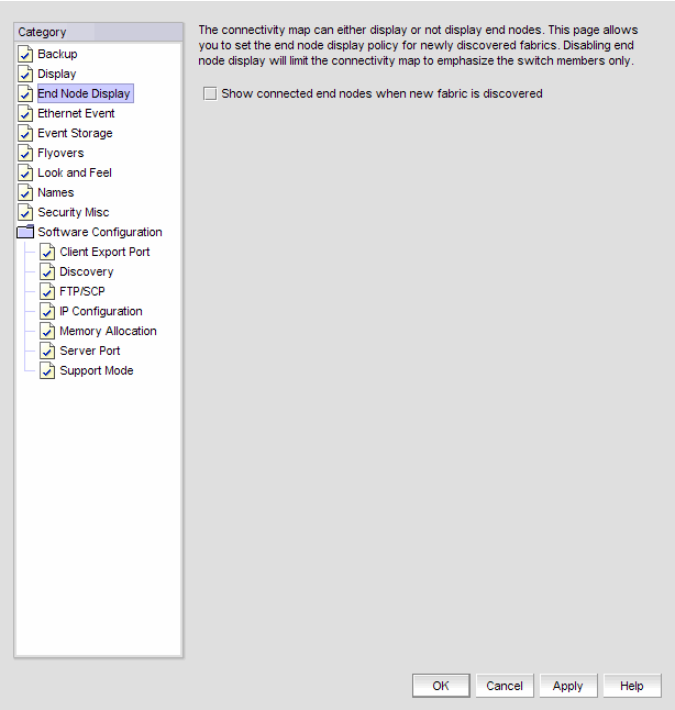


FIGURE 27 Options Dialog Box (End Node Display option)

2. Select **End Node Display** in the **Category** list.
3. Select the **Show connected end nodes when new fabric is discovered** check box to display end nodes on your system.

   NOTE
   Before changes can take effect, the topology must be rediscovered.

4. Click **Apply** or **OK** to save your work.

Ethernet events

An Ethernet event occurs when the Ethernet link between the Management Server and the managed device is lost. You can configure the application to enable events when the Ethernet connection is lost.

Enabling Ethernet events

The **Options** dialog box enables you to configure the Management application to generate an Ethernet event after a device is offline for a specific period of time.

To enable Ethernet events, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 28).

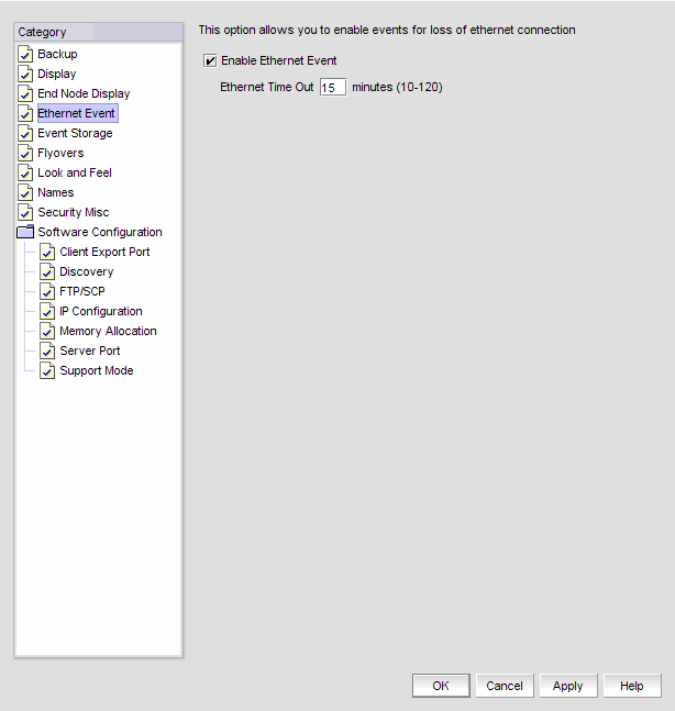


FIGURE 28 **Options Dialog Box (Ethernet Event option)**

2. Select **Ethernet Event** in the **Category** list.
3. Select the **Enable Ethernet Event** check box.
4. Enter the Ethernet time out value (10 to 120 minutes).
5. Click **Apply** or **OK** to save your work.

Disabling Ethernet events

To disable Ethernet events, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Ethernet Event** in the **Category** list.
3. Clear the **Enable Ethernet Event** check box.
4. Click **Apply** or **OK** to save your work.

Event storage

You can configure the number of historical events in the repository as well as how long the events will be retained.

Configuring event storage

To configure event storage, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 29).

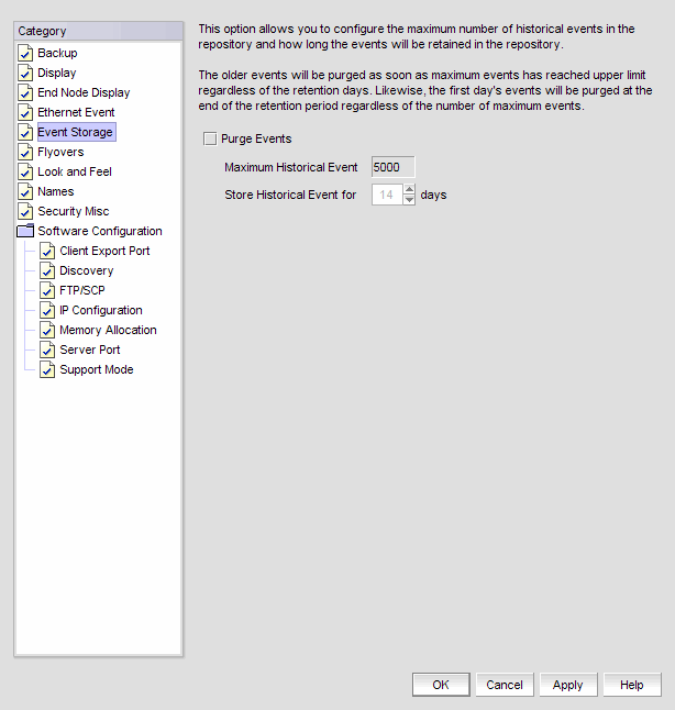


FIGURE 29 **Options Dialog Box (Event Storage option)**

2. Select **Event Storage** in the **Category** list.

3. Select the **Purge Events** check box.
4. Enter the number of events (1 through 20000) in the repository in the **Maximum Historical Event** field.

   Older events are purged as soon as the maximum events is reached regardless of the retention days.
5. Enter then number of days (1 through 30) you want to store events in the **Store Historical Event for** <*number*> **days** field.

   The events are purged at the end of the retention period regardless of the number of maximum events.
6. Click **OK**.

Flyovers

You can configure your system to display information for products and connections in a pop-up window on the Connectivity Map.

Configuring flyovers

To display product information in a pop-up window, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.
2. Select **Flyovers** in the **Category** list.
3. Select the **Enable flyover display** check box to enable flyover display on your system.
4. Select the **Include labels** check box to include labels on flyover displays.

5. Select the **Product** tab (Figure 31) and complete the following steps to select the product properties you want to display on flyover.

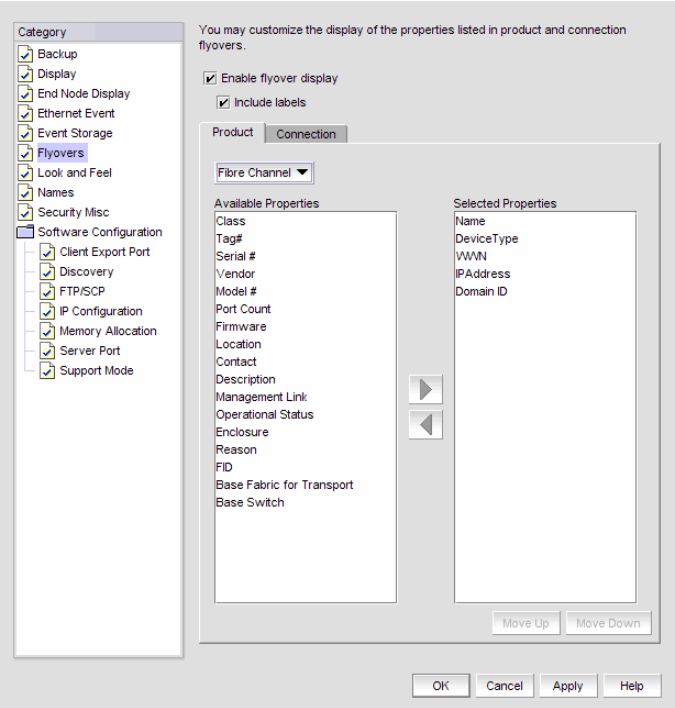


FIGURE 30 **Options Dialog Box (Flyovers option, Product tab)**

a. Select each property you want to display in the product flyover from the **Available Properties** table.

The available product properties include the following options:

- Name
- Device Type
- WWN
- IP Address
- Domain ID
- Class
- Tag#
- Serial #
- Vendor
- Model #
- Port Count
- Seed Switch
- Firmware
- Location
- Contact
- Description
- Management Link
- Operational Status
- Enclosure
- Reason
- FID
- Base Fabric for Transport
- Base Switch

b. Click the right arrow to move the selected properties to the **Selected Properties** table.

c. Use the **Move Up** and **Move Down** buttons to reorder the properties in the **Selected Properties** table, if necessary.

The properties displayed in the **Selected Properties** table appear in the flyover display.

6. Select the **Connection** tab (Figure 31) and complete the following steps to select the information you want to display on flyover.

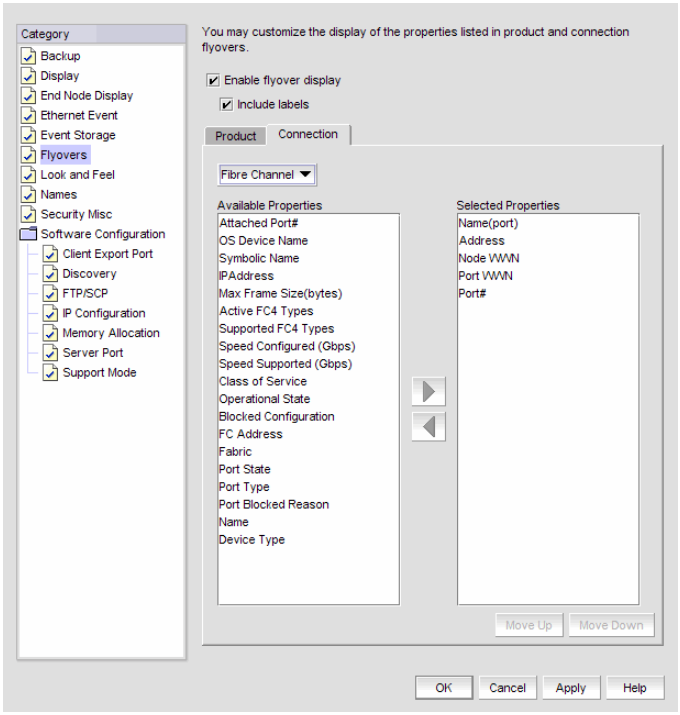


FIGURE 31 Options Dialog Box (Flyovers option, Connection tab)

a. Select the protocol from the **Protocol** list.

   The default protocol is Fibre Channel. Depending on which protocol you select, some properties may not be available for all protocols.

b. Select each property you want to display in the connection flyover from the **Available Properties** table.

   Depending on which protocol you select, some of the following properties may not be available for all protocols:

   Fibre Channel (default)

   - Name (port)
   - Address
   - Node WWN
   - Port WWN
   - Port#
   - Attached Port#
   - OS Device Name
   - Symbolic Name
   - IP Address
   - Max Frame Size (bytes)
   - Active FC4 Types
   - Supported FC4 Types
   - Speed Configured (Gbps)
   - Speed Supported (Gbps)
   - Class of Service
   - Operational State
   - Blocked Configuration
   - FC Address
   - Fabric
   - Port State
   - Port Type
   - Port Blocked Reason
   - Name
   - Device Type

FCoE

- Name
- Node WWN
- MAC
- Port#
- Port Type
- FCoE Index #

c. Click the right arrow to move the selected properties to the **Selected Properties** table.

d. Use the **Move Up** and **Move Down** buttons to reorder the properties in the **Selected Properties** table.

   The properties displayed in the **Selected Properties** table appear in the flyover display.

7. Click **Apply** or **OK** to save your work.

Turning flyovers on or off

Flyovers display when you place the cursor on a product. They provide a quick way to view a product's properties.

To turn flyovers on or off, select **Enable Flyover Display** from the **View** menu.

Viewing flyovers

On the Connectivity Map, rest the pointer over a product icon, port, or connection.

The pop-up window containing the product, port, or connection information displays.

Names

You can use Names as a method of providing familiar simple names to products and ports in your SAN. Using your Management application you can:

- Set names to be unique or non-unique.
- Fix duplicate names.
- Associate a name with a product or port WWN currently being discovered.
- Add a WWN and an associated name for a product or port that is not yet being discovered.
- Remove or disassociate a name from a WWN.

Setting names to be unique

You can edit duplicate names so that each device has a unique name. Note that the **Duplicated Names** dialog box only displays when you set names to be unique and there are duplicate names in the system.
To edit duplicate names, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 32).

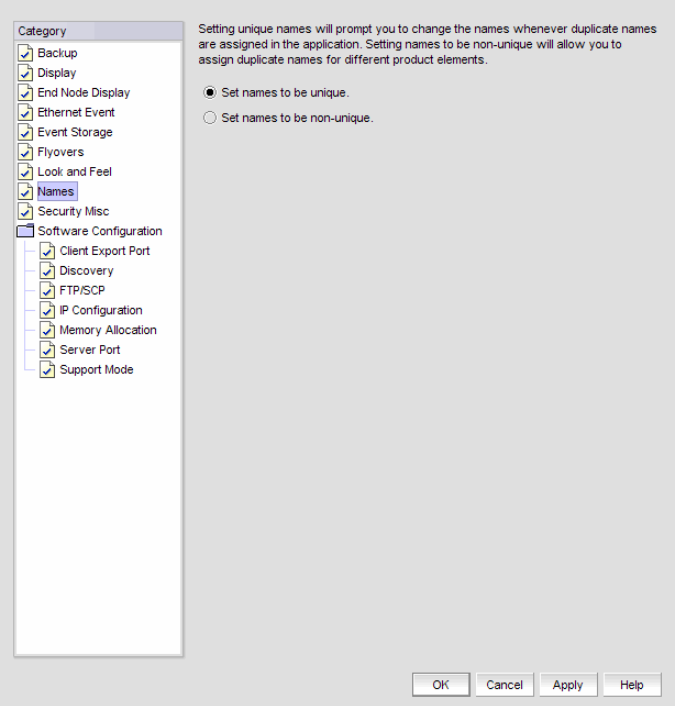


FIGURE 32 **Options Dialog Box (Names option)**

2. Select **Names** in the **Category** list.
3. Select **Set names to be unique** to require that names be unique on your system.
4. Click **OK** on the **Options** dialog box.
5. Click **OK** on the “duplicate names may exist” message.
   To fix duplicated names, refer to “Fixing duplicate names” on page 88.

Setting names to be non-unique

You can choose to allow duplicate names in your fabric.

To set names to be non-unique, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Names** in the **Category** list.
3. Select **Set names to be non-unique** to allow duplicate names on your system.
4. Click **OK** on the **Options** dialog box.

Fixing duplicate names

To fix duplicated names, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays (Figure 33).

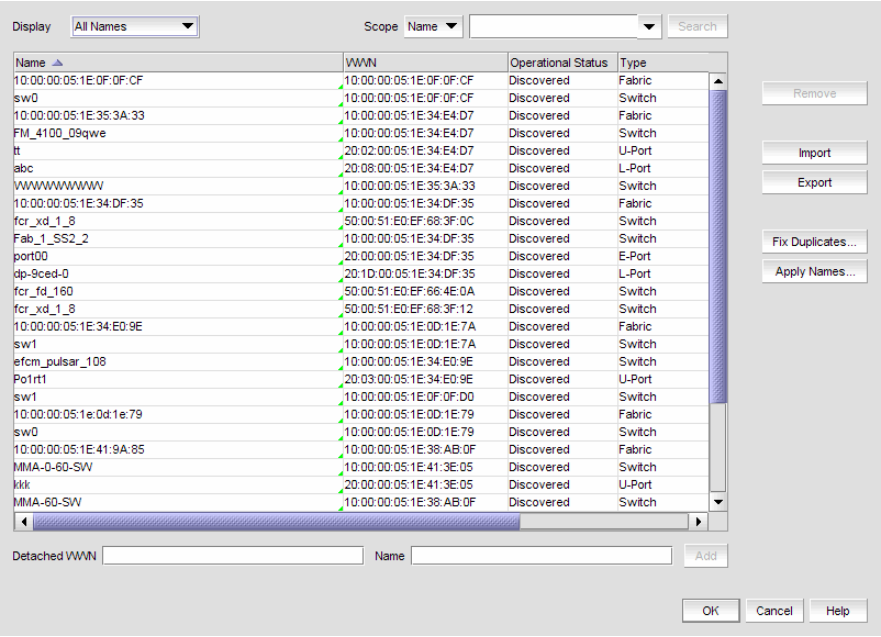


FIGURE 33 Configure Names Dialog Box

2. Click **Fix Duplicates**.

   The **Duplicated Names** dialog box displays.

3. Select one of the following options.

   - If you select **Append Incremental numbers for all repetitive names**, the names are edited automatically using incremental numbering.
   - If you select **I will fix them myself**, edit the name in the **Name** field.

4. Click **OK** on the **Duplicated Names** dialog box.

5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Viewing names

To view names associated with devices by name, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.

   Only devices with a name display. The table displays the Name, WWN, Operational Status, Type, and a Description of the device.

3. Click **OK** to close the **Configure Names** dialog box.

Adding a name to an existing device

To add a name to an existing device, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Select how you want to display devices from the **Display** list.

   You can display devices by **All Names**, **All WWNs**, **Only Fabrics**, **Only Products**, **Only Ports**, or **Switch and N Ports**.

   All discovered devices display.

3. Select the device to which you want to assign a name in the **Display** table.
4. Double-click in the **Name** column for the selected device and enter a name for the device.

   If you set names to be unique on the **Options** dialog box and the name you entered already exists, the entry is not accepted.

   NOTE
   If you segment a fabric, the Fabric's name follows the assigned principal switch.

5. Click **OK** on the confirmation message.
6. Click **OK** to close the **Configure Names** dialog box.

Adding a name to a new device

To add a new device and name it, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Enter the WWN of the device in the **Detached WWN** field.
3. Enter a name for the device in the **Name** field.
4. Click **Add**.

   The new device displays in the table.

   If you set names to be unique on the **Options** dialog box and the name you entered already exists, a message indicating the name already in use displays. Click **OK** to close the message and change the name.

5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Removing a name from a device

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. In the **Display** table, select the name you want to remove.
3. Click **Remove**.

   An application message displays asking if you are sure you want clear the selected name.

4. Click **Yes**.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Editing names

To edit the name associated with a device, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.

   Only devices with a name display. The table displays the Name, WWN, Operational Status, Type, and a Description of the device.

3. Click the name you want to edit in the **Name** column.
4. Edit the name and press **Enter**.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Exporting names

To export the names associated with devices, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Click **Export.**

   The **Export Files** dialog displays.

3. Browse to the location where you want to save the export file.
4. Enter a name for the file and click **Save.**
5. Click **OK** to close the **Configure Names** dialog box.

Importing Names

If the name length exceeds the limitations detailed in the following table, you must edit the name (in the CSV file) before import. Names that exceed these limits will not be imported. If you migrated from a previous version, the .properties file is located in the <Install_Home>\migration\data folder.

TABLE 17 Name limitations

Device	Character limit
Fabric OS switch 6.2 or later	30
Fabric OS switch 6.1.X or earlier	15
Fabric OS switch port	32
Others names	128

To import names, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Click **Import.**

   The **Import Files** dialog displays.

3. Browse to the import (.csv) file location.
4. Select the file and click **Import.**
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Searching by name

You can search for objects (switch, fabric, product, ports, or N Ports) by name.

To search by name, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.
3. Select **Name** from the **Scope** list.
4. Enter the name you want to search for in the **Search** field.

   You can search on partial names.

5. Click **Search**.

   All devices with the specified name (or partial name) are highlighted in the **Display** table. You may need to scroll to see all highlighted names.

6. Click **OK** to close the **Configure Names** dialog box.

Searching by WWN

You can search for objects (switch, fabric, product, ports, or N Ports) by WWN (world wide name).

To search by WWN, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.
3. Select **WWN** from the **Scope** list.
4. Enter the WWN you want to search for in the **Search** field.

   You can search on partial WWNs.

5. Click **Search**.

   All devices with the specified WWN (or partial WWN) are highlighted in the **Display** table. You may need to scroll to see all highlighted WWNs.

6. Click **OK** to close the **Configure Names** dialog box.

Security

You can configure the Server Name, CHAP secret value, and login banner, and modify whether or not to allow clients to save passwords. When the login banner is enabled, each time a client connects to the server, the login banner displays with a legal notice provided by you. The client's users must acknowledge the login banner to proceed, otherwise they are logged out.

Configuring the server name

To set the CHAP secret, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 34).

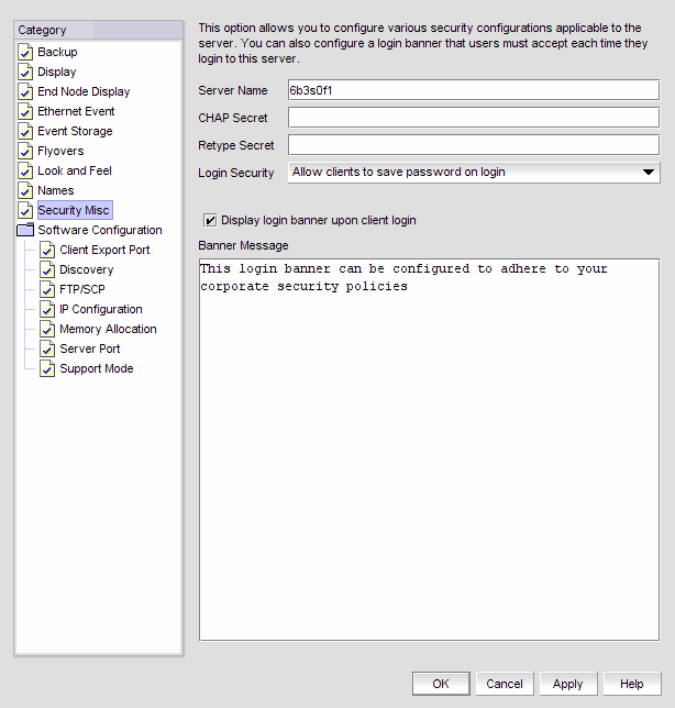


FIGURE 34 Options Dialog Box (Security Misc option)

2. Select **Security Misc** in the **Category** list.
3. Enter the server name in the **Server Name** field.

   The **Server Name** field cannot be empty.
4. Enter a password in the **CHAP Secret** field.

   The secret must be entered as a 32-digit hexadecimal value, or as a 16-digit ASCII value preceded by a dollar sign ($), for example, $abcdefghijklmnop.

5. Re-enter the password in the **Retype Secret** field.

   If the secret does not meet the application requirements or the **CHAP Secret** and **Retype Secret** entries do not match, an error message displays. Click **OK** to re-enter the **CHAP Secret** and **Retype Secret** values.

   You are about to modify the ID/Secret of this server. Check all products that this server is managing and make sure the corresponding Software ID/Secret is updated appropriately. If you fail to do so, your server may not be able to manage the products any more.

6. Click **OK** on the confirmation message.
7. Click **Apply** or **OK** to save your work.

Setting the CHAP secret

To set the CHAP secret, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Enter a password in the **CHAP Secret** field.

   The secret must be entered as a 32-digit hexadecimal value, or as a 16-digit ASCII value preceded by a dollar sign ($), for example, $abcdefghijklmnop.

4. Re-enter the password in the **Retype Secret** field.

   If the secret does not meet the application requirements or the **CHAP Secret** and **Retype Secret** entries do not match, an error message displays. Click **OK** to re-enter the **CHAP Secret** and **Retype Secret** values.

   You are about to modify the ID/Secret of this server. Check all products that this server is managing and make sure the corresponding Software ID/Secret is updated appropriately. If you fail to do so, your server may not be able to manage the products any more.

5. Click **OK** on the confirmation message.
6. Click **Apply** or **OK** to save your work.

Configuring login security

To configure login security, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Choose one of the following options:
   - To allow users to save their password in the **Login Security** list, select **Allow clients to save password on login**.
   - To not allow users to save their password in the **Login Security** list, select **Do NOT allow clients to save password on login**.
4. Click **Apply** or **OK** to save your work.

Configuring the login banner display

To configure the login banner display, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Select the **Display login banner upon client login** check box.
4. Enter the message you want to display every time a user logs into this server in the **Banner Message** field.

   This field contains a maximum of 1024 characters.

5. Click **Apply** or **OK** to save your work.

Disabling the login banner

To disable the login banner display, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Clear the **Display login banner upon client login** check box.

   NOTE
   Users logging into the client will not see the banner when logging in to this Server.

4. Click **Yes** on the confirmation message.
5. Click **Apply** or **OK** to save your work.

Software Configuration

The Management application allows you to configure the following software settings:

- Client export port—A port for communication between the client and server.
- Discovery—HTTP or HTTP over SSL when connecting to the switch.
- FTP/SCP overview—Internal or external FTP server settings.
- IP Configuration—Configure the Ethernet ports with the IP address.
- Memory allocation—Memory allocation for the client and server.
- Server port—Server port settings.
- Support mode—Support settings to allow enhanced diagnostics.

Client export port

You can configure a port for communication between the client and server.

Configuring the client export port

To configure client export port settings, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 35).

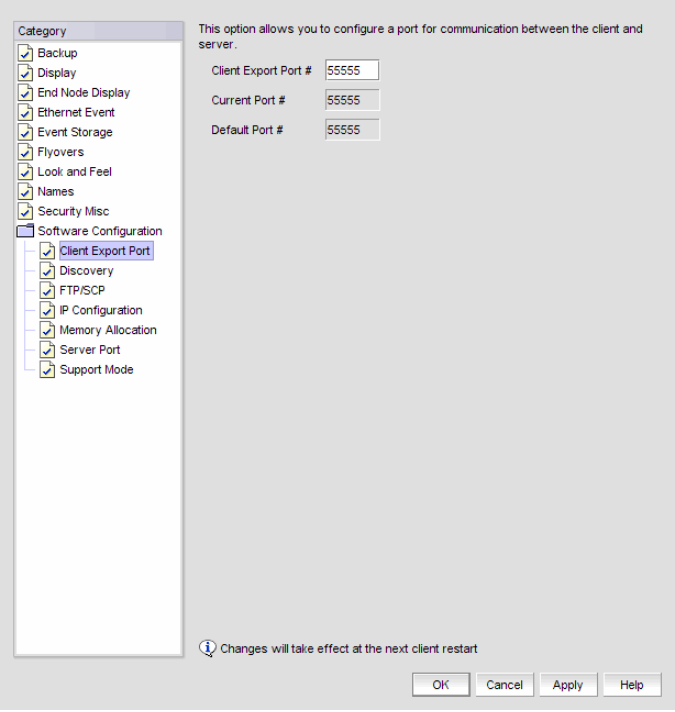


FIGURE 35 **Options Dialog Box (Client Export Port option)**

2. Select **Client Export Port** to assign a communications port between the client and server in the **Category** list.

3. Enter the client export port number to set a fixed port number for the client in the **Client Export Port** field.
4. Click **Apply** or **OK** to save your work.

NOTE
Changes to this option take effect after a client restart.

5. Click **OK** on the "changes take effect after client restart" message.

Discovery

You can configure connections between the switch and the Management application server.

Configuring Discovery

To configure discovery, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 36).

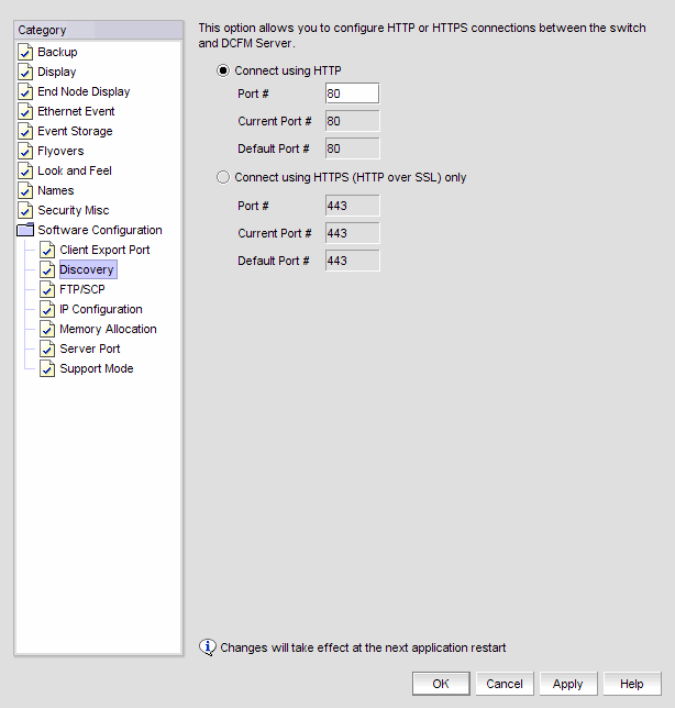


FIGURE 36 **Options Dialog Box (Discovery option)**

2. Select **Discovery** in the **Category** list.

3. Choose one of the following options:
   - If you want to connect using HTTP, complete the following steps.
     a. Select the **Connect using HTTP** option.
     a. Enter the connection port number in the **Port #** field. Continue with step 4.
   - If you want to connect using HTTPS (HTTP over SSL), complete the following steps.
     a. Select the **Connect using HTTPS (HTTP over SSL) only** option.
     b. Enter the connection port number in the **Port #** field. Continue with step 4.
4. Click **Apply** or **OK** to save your work.

NOTE
Changes to this option take effect after an application restart.

5. Click **OK** on the "changes take effect after application restart" message.

FTP/SCP overview

File Transfer Protocol (FTP) is a network protocol used to transfer data from one computer to another over a TCP computer network. During installation, a built-in FTP server and its services are installed. Other FTP servers on your system are recognized by the application as external FTP servers.

For Windows systems, the built-in FTP server is the default configuration and installation starts the FTP service if port 21 is not used by any other FTP server. For UNIX systems, built-in FTP is the default for UNIX systems during installation; the external FTP server is the default only if port 21 is busy.

Note that when uninstalling the application the built-in FTP server is removed with all other services even if the FTP service is used by firmware upgrade or supportSave features.

Secure Copy (SCP) is a means of securely transferring computer files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol. You must configure SCP on your machine to support Technical Support and firmware download.

Accessing the FTP server folder

Choose from one of the following options to access the FTP server folder:

- To access the internal FTP folder, select **Monitor > Techsupport > View Repository**.
- To access the external FTP folder, type the following in a browser window:
  ftp://<*Username*>@<*External_FTP_Server_IP_Address*>
  (for example, ftp://admin@10.1.1.1) and press **Enter**. Type your password in the pop-up window and press **Enter**. The external FTP folder displays.

Configuring an internal FTP server

To configure the internal FTP server settings, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 37).

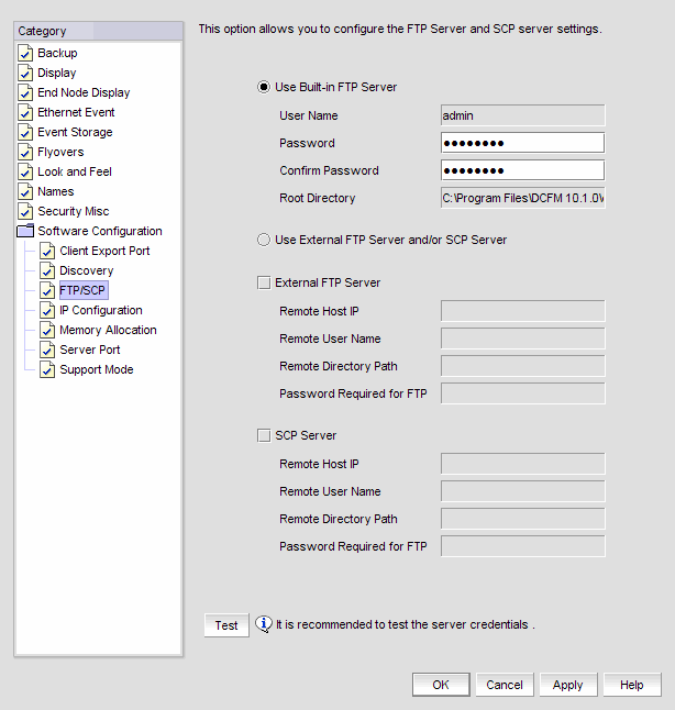


FIGURE 37 Options Dialog Box (FTP/SCP option)

2. Select **FTP/SCP** in the **Category** list.
3. Select the **Use built-in FTP Server** option to use the default built-in FTP server.

   All active fields are mandatory.
4. Change your password by entering a new password in the **Password** and **Confirm Password** fields.
5. Click **Test** to test the FTP server.

   An “FTP Server running successfully” or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.
6. Click **Apply** or **OK** to save your work.

Configuring an external FTP server

To configure the external FTP server settings, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **FTP/SCP** in the **Category** list.
3. Select the **Use External FTP Server and/or SCP Server** option.
4. Select the **External FTP Server** check box to configure the external FTP server.

   All fields are mandatory.

5. Enter the IP address for the remote host in the **Remote Host IP** field.
6. Enter a user name in the **Remote User Name** field
7. Enter the path to the remote host in the **Remote Directory Path** field.

   Use a slash (/) or a period (.) to denote the relative root directory of the FTP server. Do not give an absolute path.

8. Enter the password in the **Password Required for FTP** field.
9. Click **Test** to test the FTP server.

   An “FTP Server running successfully” or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

10. Click **OK** on the message.
11. Click **Apply** or **OK** to save your work.

Configuring a FTP or SCP server

To configure the SCP server settings, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **FTP/SCP** in the **Category** list.
3. Select the **Use External FTP Server and/or SCP Server** option.
4. Select the **FTP Server** check box to configure the external FTP server.

   All fields are mandatory.

5. Enter the IP address for the remote host in the **Remote Host IP** field.
6. Enter a user name in the **Remote User Name** field.
7. Enter the path to the remote host in the **Remote Directory Path** field.

   Use a slash (/) or period (.) to denote the root directory. Do not give an absolute path.

8. Enter the password in the **Password Required for FTP** field.

9. Click **Test** to test the FTP server.

   A "Server running successfully" or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

10. Click **OK** on the message.
11. Click **Apply** or **OK** to save your work.

Testing the FTP and SCP server

To test the FTP and SCP server, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **FTP/SCP** in the **Category** list.
3. Choose one or more of the following options:

   - If you are using the internal FTP server, select the **Use built-in FTP Server** option.

     For step-by-step instructions about configuring the built-in server, refer to "Configuring an internal FTP server" on page 99.

   - If you are using the external FTP server, select the **Use External FTP Server** option.

     For step-by-step instructions about configuring the built-in server, refer to "Configuring an external FTP server" on page 100.

4. Click **Test**.

   An "FTP or SCP Server running successfully" or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

5. Click **OK** on the message.
6. Click **OK** to close the **Options** dialog.

IP Configuration

You can configure IP Configuration settings.

Configuring IP Configuration settings

NOTE
The server binds using IPv6 address by default if your Operating System is IPv6-enabled (dual mode or IPv6 only). The server binds using IPv4 address by default if your Operating System is IPv4-enabled. Servers running in dual mode allow the client to communicate from both IPv6 and IPv4 addresses.

To configure the IP address used by the server for client-server communications, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 38).

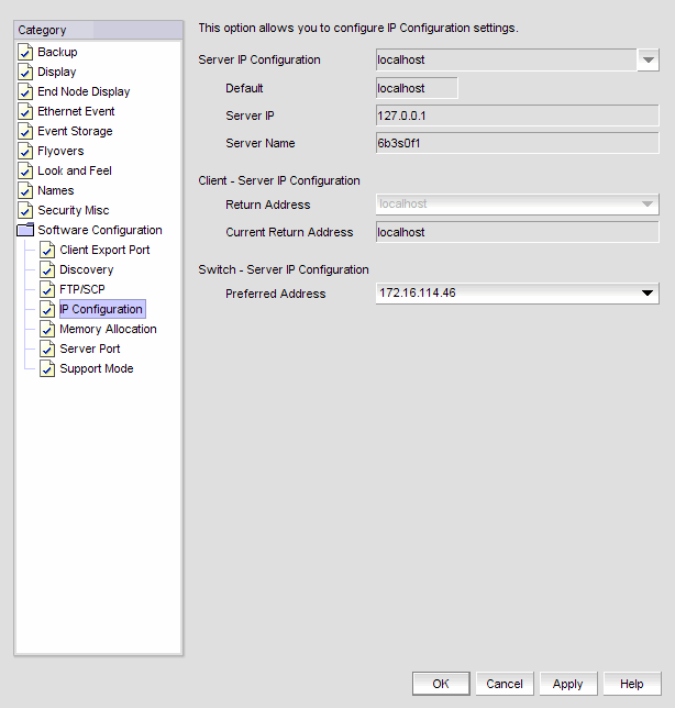


FIGURE 38 **Options Dialog Box (IP Configuration option)**

2. Select **IP Configuration** in the **Category** list to set the IP address.
3. Select the preferred IP address in the **Switch - Server IP Configuration Preferred Address** list.

   If DNS is not configured for your network, do not select the 'hostname' option from either the **Return Address** or **Preferred Address** list. Selecting the 'hostname' option prevents clients and devices from communicating with the Server.
4. Click **Apply** or **OK** to save your work.

Configuring an explicit server IP address

If you selected a specific IP address from the **Server IP Configuration** screen during installation and the selected IP address changes, you will not be able to connect to the server. To connect to the new IP address, you must manually update the IP address information.

If the client-to-server communication IP address was configured as the 'host name', complete the following steps.

1. Open the **Server Management Console** from the **Start** menu.
2. Click the **Services** tab, if necessary, and click **Stop**.
3. Open the ftpd.properties file (located in the <Install_Home>\conf\ folder) in a text editor (such as Notepad).
4. Edit the following variables:

   `config.data-connection.active.local-address=<New_IP_Address>`

   `config.data-connection.passive.address=<New_IP_Address>`
5. Save and close the file.
6. Update the FTP_SERVER table's IP column with the <*New_IP_Address*> in the database.
7. Open the **Server Management Console** from the **Start** menu.
8. Click the **Services** tab, if necessary, and click **Start**.
9. Open the Management application from the **Start** menu.
10. Login to the application using the following steps.
    a. To open the application, double-click the desktop icon or open from the **Start** menu.

       The **Log In** dialog box displays
    b. Enter your user name and password.

       The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.
    c. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
    d. Click **Login**.
11. Configure the IP address for Switch - Server IP configuration using the following steps.
    a. Select **SAN > Options**.

       The **Options** dialog box displays
    b. Click **IP Configuration**.

       The **Options** dialog box displays
    c. Select the correct IP address from the **Switch - Server IP Configuration** list.

12. Restart the server to perform SNMP and Syslog auto registration with the new server IP address to all switches.

NOTE
If the old server IP address displays in SNMP trap and Syslog recipient list, you must manually remove it from the list. The Management application server does not remove the old server IP address during auto-registration.

If the client-to-server communication IP address was configured with a specific IP address, complete the following steps.

1. Open the **Server Management Console** from the **Start** menu.
2. Click the **Services** tab, if necessary, and click **Stop**.
3. Open the ftpd.properties file (located in the <Install_Home>\conf\ folder) in a text editor (such as Notepad).
4. Edit the following variables:

   `config.data-connection.active.local-address=<New_IP_Address>`

   `config.data-connection.passive.address=<New_IP_Address>`
5. Save and close the file.
6. Update the FTP_SERVER table's IP column with the <*New_IP_Address*> in the database.
7. Open the `<Management_Application_Name>svc.conf` file (located in the <Install_Home>\conf\ folder) in a text editor (such as Notepad).
8. Edit the following variable:

   `set.BIND_ADDRESS=<New_IP_Address>`
9. Save and close the file.
10. Open the `<Management_Application_Name>.properties` file (located in the <Install_Home>\conf\ folder) in a text editor (such as Notepad).
11. Edit the following variable:

    `java.rmi.server.hostname=<New_IP_Address>`
12. Save and close the file.
13. Open the **Server Management Console** from the **Start** menu.
14. Click the **Services** tab, if necessary, and click **Start**.
15. Login to the application using the following steps.
    a. To open the application, double-click the desktop icon or open from the **Start** menu.

       The **Log In** dialog box displays
    b. Enter your user name and password.

       The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.
    c. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
    d. Click **Login**.

16. Configure the IP address for Switch - Server IP configuration using the following steps.
    a. Select **SAN > Options**.

       The **Options** dialog box displays

    b. Click **IP Configuration**.

       The **Options** dialog box displays

    c. Select the correct IP address from the **Switch - Server IP Configuration** list.
17. Restart the server to perform SNMP and Syslog auto registration with the new server IP address to all switches.

NOTE
If the old server IP address displays in SNMP trap and Syslog recipient list, you must manually remove it from the list. The Management application server does not remove the old server IP address during auto-registration.

Memory allocation

You can configure memory allocation for the client and server to improve performance. You can trigger switch polling when a state changes or you can poll at intervals when no state change occurs.

NOTE
SAN size is a consideration in selection of polling periods.

Configuring memory allocation settings

To configure memory allocation settings, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 39).

2. Select **Memory Allocation** in the **Category** list to set the memory allocation for the server and client.

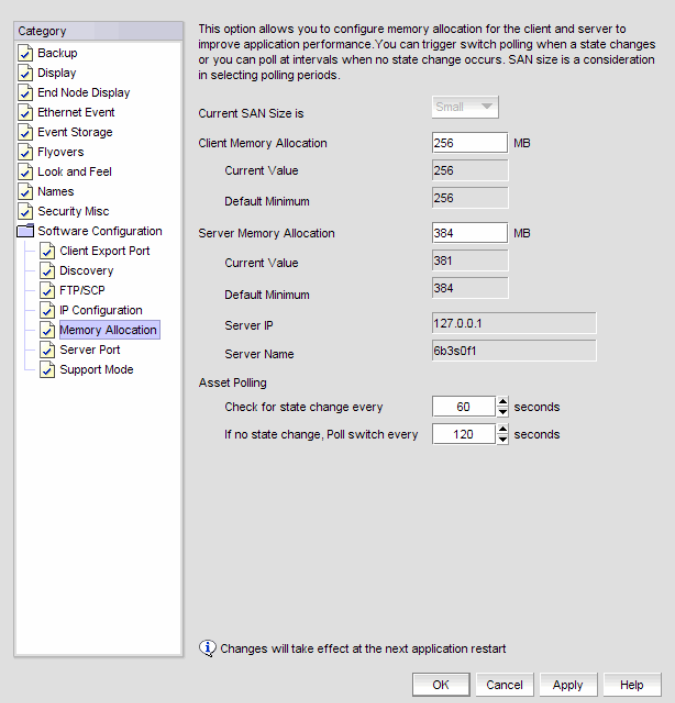


FIGURE 39 Options Dialog Box (Memory Allocation option)

3. Enter the memory allocation (MB) for the client in the **Client Memory Allocation** field.

   If you enter an invalid value, an error message displays with the minimum value (256 MB) allowed. Click **OK** and edit the value again.

4. Enter the memory allocation (MB) for the server in the **Server Memory Allocation** field.

   If your server has a minimum of 2 Gb RAM, change the default server memory value to 1024 MB. If your server is running less than 2 Gb RAM, do not change the default (512 MB).

   Do not exceed the following server memory values:

   - For Windows systems, the maximum server memory allocation is 1.4 GB.
   - For UNIX systems, the maximum server memory allocation is 2 GB.

   If you enter an invalid value, an error message displays with the minimum value (768 MB) allowed. Click **OK** and edit the value again.

5. Click **Apply** or **OK** to save your work.

   NOTE
   Changes to this option take effect after an application restart.

6. Click **OK** on the "changes take effect after application restart" message.

Configuring asset polling

To configure asset polling, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Memory Allocation** in the **Category** list to set the memory allocation for the server and client.

3. Enter how often (default is 60 seconds) you want to check for state changes in the **Check for state change every** field.

   You cannot enter a vaule lower than the default minimum value.

4. Enter how often (default is 120 seconds) you want to check for state changes in the **If no state change, Poll switch every** field.

5. Click **Apply** or **OK** to save your work.

   NOTE
   Changes to this option take effect after an application restart.

6. Click **OK** on the "changes take effect after application restart" message.

Server port

You can configure the server port settings so that you can assign a web server port number and set the server port to be SSL-enabled.

Configuring the server port

To configure server settings, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 40).

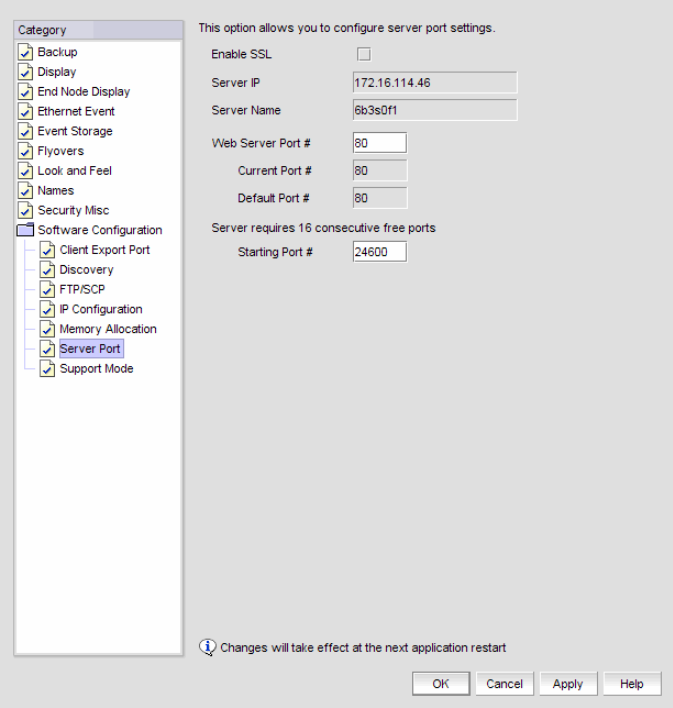


FIGURE 40 Options Dialog Box (Server Port option)

2. Select **Server Port** in the **Category** list.
3. Select the **Enable SSL** check box to enable this function for the server port.
4. Enter a port number in the **Web Server Port #** field.

   NOTE
   Do not use port 2638 for any of these port numbers. Port 2638 is used internally by the server.

5. Enter a port number in the **Starting Port #** field.

   The server requires 13 consecutive free ports beginning with the starting port number.

6. Click **Apply** or **OK** to save your work.

NOTE
Changes to this option take effect after application restart.

7. Click **OK** on the “changes take effect after application restart” message.

Support mode

You can configure support settings to allow enhanced diagnostics.

Configuring support mode settings

To configure support mode settings, complete the following steps.

1. Select **SAN > Options**.

   The **Options** dialog box displays (Figure 41).

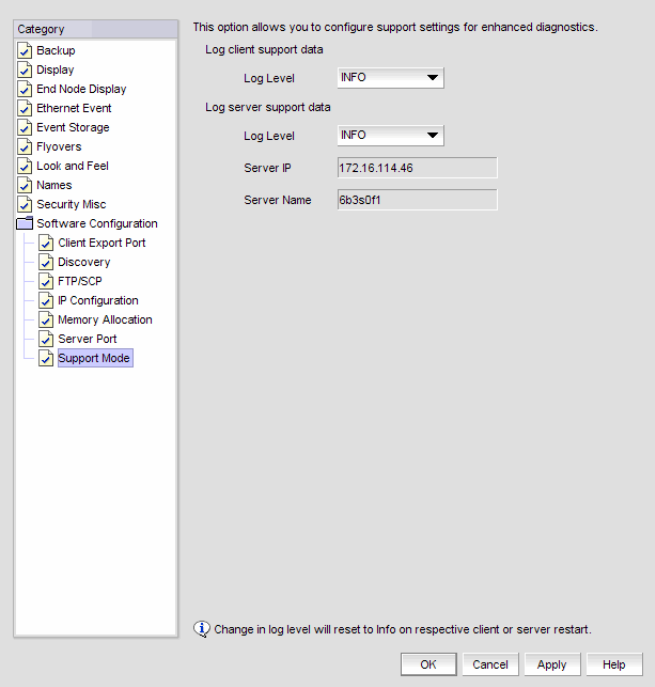


FIGURE 41 Options Dialog Box (Support Mode option)

2. Select **Support Mode** in the **Category** list to enable or disable support modes.

NOTE
Only use this option when directed to by customer support.

3. Select the **Log client support data - Log Level** list, and select the type of log data you want to configure.

   Log level options include: **All**, **Fatal**, **Error**, **Warn**, **Info**, **Debug**, **Trace**, and **Off**. Default is **Info**.

   The log level options return to the default value (Info) when the client or server is restarted.

4. Select the **Log server support data - Log Level** list, and select the type of log data you want to configure.

   Log level options include: **All**, **Fatal**, **Error**, **Warn**, **Info**, **Debug**, **Trace**, and **Off**. Default is **Info**.

5. Click **Apply** or **OK** to save your work.

   Each log file (except the server log file) is limited to 5 MB. The server log file is limited to 10 MB. When a file reaches the maximum size, and there are less than 10 files for the server or 5 files for the client, a new file is created.

   For web clients, log files (client.log.1 through client.log.5) are created in the <*Install_Home*>\<*Server_Name*> directory.

   For clients, log files (client.log.1 through client.log.5) are created in the <*User_Home*> directory.

   For servers, log files (server.log.1 through server.log.10) are created in the <*User_home*>\jboss\server\dcm\log directory.

Fabric tracking

When you discover a new fabric and initial discovery is complete, fabric tracking is automatically enabled. Subsequently, if a switch or end-device is added to or removed from the fabric, a plus (+) or minus (-) icon displays (see table below) next to the product icon. Connections are also tracked. A new connection displays a solid gray line with a added icon and missing connections display a yellow dashed line with a removed icon.

TABLE 18 Fabric Tracking Icons

	Device Added
	Device Removed

Enabling fabric tracking

To enable fabric tracking, choose from one of the following options:

- Select a fabric on the Product List or Connectivity Map and select **Monitor > Track Fabric Changes**.
- Right-click a fabric on the Product List or Connectivity Map and select **Track Fabric Changes**.

Disabling fabric tracking

To disable fabric tracking, choose from one of the following options:

- Select the fabric on which you want to disable fabric tracking on the Product List or Connectivity Map and select **Monitor > Track Fabric Changes**.
- Right-click the fabric on which you want to disable fabric tracking on the Product List or Connectivity Map and select **Track Fabric Changes**.

Accepting changes for a fabric

To accept all changes to a fabric, choose from one of the following options:

- Select a fabric on the Product List or Connectivity Map and select **Monitor > Accept Changes**.
- Right-click a fabric on the Product List or Connectivity Map and select **Accept Changes**.

  The added and removed icons and the missing connection dotted yellow line are cleared from the display.

Accepting changes for a device

To accept the changes to a device, choose from one of the following options:

- Select the device on the Product List or Connectivity Map and select **Monitor > Accept Changes**.
- Right-click the device on the Product List or Connectivity Map and select **Accept Change**.

  The added or removed icon is cleared from the display.

Third-party tools

You can open other software products you frequently use from the **Tools** menu or shortcut menus.

Starting third-party tools from the application

You can open third-party tools from the **Tools** menu or a device's shortcut menu. Remember that you cannot open a tool that is not installed on your computer.

NOTE
Installing tools is only available with the Enterprise Edition.

To open an application, perform the following steps.

1. Select the device.
2. Use one of the following techniques:
   - Select **Tools > Product Menu >** <*Tool_Name*>.
   - Select **Tools >** <*Tool_Name*>.
   - Right-click the device, and select the tool from the menu.

Launching a Telnet session

You can use Telnet to log in and issue command line-based commands to a switch.

NOTE
The switch must have a valid IP address. If the device does not have a valid IP address, the Telnet selection will not be available on the **Tools** menu or the shortcut menu. You must right-click the device icon, select **Properties,** and enter the device's IP address before you can open a Telnet session.

To launch a telnet session, complete the following steps.

On the Connectivity Map, right-click a device and select **Telnet** or **Telnet through Server**.

NOTE
Telnet through Server is only supported on Windows systems.

OR

1. Select the switch to which you want to connect.
2. Select **Tools > Product Menu > Telnet**.

   The Telnet session window displays.

   NOTE
   On Linux systems, you must use CTRL + BACKSPACE to delete text in the Telnet session window.

Launching an Element Manager

Element Managers are used to manage Fibre Channel switches and directors. You can open a device's Element Manager directly from the application.

To launch a device's Element Manager, complete the following steps.

On the Connectivity Map, double-click the device you want to manage.

The Element Manager displays.

OR

On the Connectivity Map, right-click the device you want to manage and select **Element Manager > Hardware**.

The Element Manager displays.

OR

1. Select a device.
2. Select **Configure > Element Manager > Hardware**.

   The Element Manager displays.

Launching Web Tools

Use Brocade Web Tools to enable and manage Brocade Access Gateway, Switches, and Directors. You can open Web Tools directly from the application. For more information about Web Tools, refer to the *Brocade Web Tools Administrator's Guide.* For more information about Brocade Access Gateway, Switches, and Directors, refer to the documentation for the specific device.

To launch a device's Element Manager, complete the following steps.

NOTE
You must have Device Administration privileges for the selected device to launch Web Tools. If you do not have Device Administration privileges, you will need to enter those credentials to launch Web Tools.

On the Connectivity Map, right-click the Fabric OS device you want to manage and select **Element Manager > Hardware**.

Web Tools displays.

OR

1. Select a Fabric OS device.
2. Select **Configure > Element Manager > Hardware**.

   Web Tools displays.

Launching FCR configuration

Use FCR Configuration to launch the FC Routing module, which enables you to share devices between fabrics without merging the fabrics. You can open the FC Routing module directly from the Management application. For more information about FC Routing, refer to the *Brocade Web Tools Administrator's Guide*.

The FCR Configuration option is available only for the following devices with Fabric OS 5.0 or later:

- Fabric OS extension switch
- Fabric OS Directors configured with an extension blade
- Fabric OS 1U, 40-port, 8 Gbps FC Switch (with Integrated Routing license)
- Fabric OS 2U, 80-port, 8 Gbps FC Switch (with Integrated Routing license)
- Fabric OS directors configured with a FC 8 GB 16-port Blade (with Integrated Routing license)
- Fabric OS directors configured with a FC 8 GB 32-port Blade (with Integrated Routing license)
- Fabric OS directors configured with a FC 8 GB 48-port Blade (with Integrated Routing license)

  Note that on the FC 8 GB 48-port Blade, the Shared Area ports, for example, 16-47, cannot be configured as EX_ports

On the Connectivity Map, right-click the Fabric OS device you want to configure and select **Element Manager > Router Admin**.

OR

1. Select a Fabric OS device.
2. Select **Configure > Element Manager > Router Admin**.

   The FC Routing module displays.

Launching HCM Agent

Use Brocade HCM Agent to enable and manage Brocade HBAs. You can open HCM Agent directly from the application. For more information about HCM Agent, refer to the *Brocade HCM Agent Administrator's Guide.* For more information about Brocade HBAs, refer to the documentation for the specific device.

To launch a device's Element Manager, complete the following steps.

NOTE
You must have Device Administration privileges for the selected device to launch HCM Agent. If you do not have Device Administration privileges, you will need to enter those credentials to launch HCM Agent.

On the Connectivity Map, right-click the Fabric OS device you want to manage and select **Element Manager > Hardware**.

HCM Agent displays.

OR

1. Select a Brocade HBA.
2. Select **Configure > Element Manager > Hardware**.

   HCM Agent displays.

Topology layout

This section provides an overview of topology layout options and instructions for changing the layout. You can customize various parts of the topology, including the layout of devices and connections as well as groups' background colors, to easily and quickly view and monitor devices in your SAN.
The following menu options are available on the **View** menu. Use these options to customize the topology layout.

Map Display. Select to specify a new layout for the desktop icons, background color for groups, as well as line type for connections between icons.

Domain ID/Port #. Select to set the display domain IDs and port numbers in decimal or hex format.

Decimal. Select to display all domain IDs and port numbers in decimal format.

Hex. Select to display all domain IDs and port indexes (user port #) in hex format.

Product Label. Select to configure which product labels display.

NOTE
Changes apply to all fabrics present in the topology when the **Product Label** option is selected.

Name (Product). Displays the product name as the product label.

WWN. Displays the world wide name as the product label.

IP Address. Displays the IP Address as the product label.

Domain ID. Displays the domain ID as the product label.

Port Label. Select to configure which port labels display.

NOTE
Changes apply to the selected fabric or the fabric to which the selected item belongs.

Name. Displays the name as the port label. If the port has not been given a name, the port's WWN displays.

Port Number. Displays the port number as the port label.

Port Address. Displays the port address as the port label.

Port WWN. Displays the port world wide name as the port label.

User Port #. Displays the user's port number as the port label.

Slot/Port. Displays the slot and port as the port label for a Chassis switch and the port number for a switch.

Port Display. Select to configure how ports display.

Occupied Product Ports. Select to display the ports of the devices in the fabrics (present in the connectivity map) that are connected to other devices.

UnOccupied Product Ports. Select to display the ports of the devices (shown in the connectivity map) that are not connected to any other device.

Attached Ports. Select to display the attached ports of the target devices.

Switch to Switch Connections. Select to display the switch to switch connections. Switch to switch connections only display when the **Attached Ports** option is also selected.

Customizing the layout of devices on the topology

You can customize the layout of devices by group type or for the entire Connectivity Map. Customizing the layout makes it easier to view the SAN and manage its devices. Group types include Fabric, Host, Storage, and Switch groups. The **Map Display Layout** list varies depending on what you selected (group type or Connectivity Map).

1. Right-click a group or the Connectivity Map and select **Map Display**, then select one of the following options:
   - **Default for** <*Group_Type*>**.** Displays the devices in the default format. Group types include Fabric, Host, Storage, and Switch groups.
   - **Free Form.** Displays the devices in the default format for Switch Groups and Router Groups.
     When the **Free Form** map display layout is selected, the **Show Ports** menu command is unavailable.
   - **Fabric.** Displays the devices in the default format.
   - **Custom Grid.** Enables you to drag and drop product or group icons into a variable grid to reorganize the topology. The grid prevents icons from obscuring other icons. If enabled on a group, devices can only be moved within the group. If enabled on a fabric, groups can only be moved within the fabric. In other words, a device cannot be moved outside of its group.
   - **Square.** Displays the device icons in a square configuration.
   - **Vertical.** Displays the device icons vertically.
   - **Horizontal.** Displays the device icons horizontally.
   - **Most Connected at Center.** Displays the node that has the most connections at the center of the topology.
   - **Directional.** Displays the internal nodes in a position where they mirror the external groups to which they are connected.
2. Select the **Set as Default Layout** check box to set your selection as the default.
3. Click **OK** on the **Map Display Properties** dialog box.

Customizing the layout of connections on the topology

You can change the way inter-device connections display on the topology.

1. Right-click a group or the Connectivity Map and select **Map Display**, then select one of the following options:
   - **Straight**. Displays connections using straight lines.
   - **Orthogonal**. Displays connections in orthogonal grid lines. Disabled if **Free Form** is selected in **Map Display Layout** area.
   - **None**. Hides the connections between devices.
2. Select the **Set as Default Layout** check box to set your selection as the default.
3. Click **OK** on the **Map Display Properties** dialog box.

Changing a group's background color

You can customize the topology by changing a group's background color.

1. Right-click a group or the Connectivity Map and select **Map Display**.

   The **Map Display Properties** dialog box displays (Figure 42).

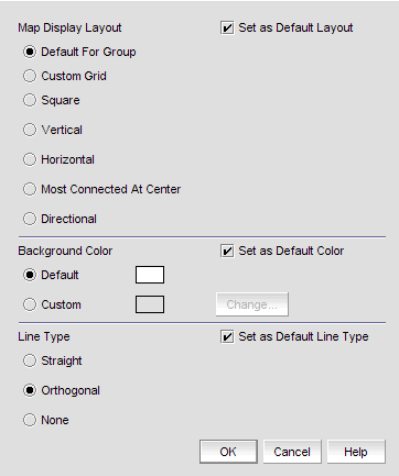


FIGURE 42 Map Display Dialog Box

2. Select the **Custom** option and click **Change**.

   The **Choose a background color** dialog box displays (Figure 43).

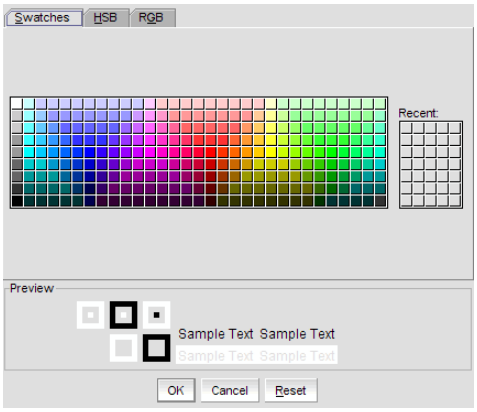


FIGURE 43 Map Display Dialog Box

3. Select or specify a color and preview it in the **Preview** pane.

   - To pick a color from a swatch, select the **Swatches** tab. Select a color from the display.
   - To specify a color based on hue, saturation, and brightness, click the **HSB** tab. Specify the hue (0 to 359 degrees), saturation (0 to 100%) and brightness (0 to 100%).
   - To specify a color based on values of red, green, and blue, click the **RGB** tab. Specify the values for red, green, and blue (0 to 255).

4. Click **OK** to change the background color, or click **Reset** to return all settings to the color currently being displayed on the topology.
5. Click **OK** on the **Map Display Properties** dialog box.

Reverting to the default background color

You can revert back to the default background color.

1. Right-click a group and select **Map Display**.

   The **Map Display Properties** dialog box displays.
2. Select the **Default** option.
3. Click **OK** on the **Map Display Properties** dialog box.

Changing the product label

1. Select a product in the Connectivity Map or Product List.
2. Select **View > Product Label**, then select one of the following options:
   - **Name (Product).** Displays the product name as the product label.
   - **WWN.** Displays the world wide name as the product label.
   - **IP Address.** Displays the IP Address as the product label.
   - **Domain ID.** Displays the domain ID as the product label.

   Changes apply to all fabrics present in the topology when the **Product Label** option is selected.

Changing the port label

1. Select a port in the Connectivity Map or Product List.
2. Select **View > Port Label,** then select one of the following options:
   - **Name.** Displays the name as the port label.
   - **Port Number.** Displays the port number as the port label.
   - **Port Address.** Displays the port address as the port label.
   - **Port WWN.** Displays the port world wide name as the port label.
   - **User Port #.** Displays the user's port number as the port label.
   - **Slot/Port.** Displays the slot and port as the port label.

   All port labels within the fabric to which the selected item belongs change to the selected port label type.

Changing the port display

You have the option of viewing connected (or occupied) product ports, unoccupied product ports, or attached ports.

NOTE
Occupied/connected ports are those that originate from a device, such as a switch. Attached ports are ports of the target devices that are connected to the originating device.

Select **View > Port Display**, then select one or more of the following options:

- **Occupied Product Ports**. Displays the ports of the devices in the fabrics (present in the connectivity map) that are connected to other devices.
- **Unoccupied Product Ports**. Displays the ports of the devices (shown in the connectivity map) that are not connected to any other device.
- **Attached Ports**. Displays the attached ports of the target devices.
- **Switch to Switch Connections**. Displays the connections between devices. Switch to switch connections only display when the **Attached Ports** option is also selected.

  All port labels on all fabrics change to the selected port label type.

Grouping on the topology

To simplify management, devices display in groups. Groups are shown with background shading and are labeled appropriately. You can expand and collapse groups to easily view a large topology.

Collapsing groups

To collapse a single group on the topology, do one of the following:

- Click the icon at the top right-hand corner of the group on the topology ( ).
- Double-click in the group, but not on a device.
- Right-click in a group, but not on a device, and select **Collapse** from the shortcut menu.

To collapse all groups on the topology by one level, click the **Collapse** button on the toolbox ( ).

Expanding groups

To expand a group on the topology, do one of the following:

- Double-click on the group icon.
- Right-click the group icon and select **Expand** from the shortcut menu.

To expand all groups on the topology by one level, click the **Expand** button on the toolbox ( ).

Viewing connections

You can view the connections in a fabric using one of the following methods:

- Select a fabric and then select **View > Connected End Devices** and select **Hide All, Show All,** or **Custom**.
- Right-click on the fabric and select **Connected End Devices > Hide All, Show All,** or **Custom**.

Configuring custom connections

NOTE
Active zones must be available on the fabric.

To create a display of the connected end devices participating in a single zone or group of zones, complete the following steps.

1. Choose from one of the following options:
   - Select a fabric on the topology and select **View > Connected End Devices > Custom**.
   - Right-click a fabric on the topology and select **Connected End Devices > Custom**.

   The **Connected End Devices - Custom display for** <*Fabric*> dialog box displays with a list of zones in the **Zones in** <*Fabric*> list.
2. Select the zones you want to include in the connection in the **Zones in** <*Fabric*> list.
3. Select the application you want to add the selected zones to in the **Application** list.
4. Click the right arrow to move them to the **Selected Zones** list.
5. Click **OK**.

Saving a custom connection configuration

NOTE
Active zones must be available on the fabric.

To save a new custom connection configuration, complete the following steps.

1. Choose from one of the following options:
   - Select a fabric on the topology and select **View > Connected End Devices > Custom**.
   - Right-click a fabric on the topology and select **Connected End Devices > Custom**.

   The **Connected End Devices - Custom display for** <*Fabric*> dialog box displays with a list of zones in the **Zones in** <*Fabric*> list.
2. Select the zones you want to include in the connection in the **Zones in** <*Fabric*> list.
3. Click the right arrow to move the selected zones to the **Selected Zones** list.
4. Click **Save**.

   The **Save Application** dialog box displays.
5. Enter a new name in the **Application Name** field.
6. Click **OK** on the **Save Application** dialog box.
7. Click **OK** on the **Connected End Devices - Custom display for** <*Fabric*> dialog box.

   The saved custom connection configuration displays in the **Connected End Devices** menu.

Deleting a custom connection configuration

NOTE
Active zones must be available on the fabric.

To delete a custom connection configuration, complete the following steps.

1. Choose from one of the following options:
   - Select a fabric on the topology and select **View > Connected End Devices > Custom**.
   - Right-click a fabric on the topology and select **Connected End Devices > Custom**.

   The **Connected End Devices - Custom display for** <*Fabric*> dialog box.
2. Select the configuration you want to delete in the **Application** list.
3. Click **Delete**.
4. Click **OK** on the confirmation message.
5. Click **OK** on the **Connected End Devices - Custom display for** <*Fabric*> dialog box.

Chapter

4

Server Management Console

In this chapter

- Server management console overview 123
- Services 124
- Changing server port numbers 126
- Restoring the database 127
- Capturing technical support information 128
- Upgrading HCM on the Management server 129

Server management console overview

Server Management Console (SMC) is an automatically installed, stand-alone application for managing the Management application server. You can perform the following tasks using the SMC:

- From the **Services** tab, you can start, stop, refresh, and restart services on the server.
- From the **Ports** tab, you can change the Management application server or web server port number.
- From the **Authentication** tab (Enterprise Edition only), you can configure an authentication server (LDAP or Radius server), and establish authentication policies.
- From the **Restore** tab, you can restore server application data.
- From the **Technical Support Information** tab, you can collect information for technical support.
- From the **HCM Upgrade** tab, you can upgrade the Management application to use a new version of Host Connectivity Manager (HCM).

Launching the SMC on Windows

Open the **Server Management Console** from the **Start** menu on the Management application server.

You can also drag the SMC icon onto your desktop as a short cut.

Launching the SMC on Linux and Solaris

Perform the following steps to launch the server management console on Linux and Solaris systems.

1. On the Management application server, go to the following directory:

   <Install DIR>*/bin*

2. Type the following at the command line:

   `./smc`

Services

You must be logged in at the administrator (Windows systems) or root (UNIX systems) level to stop, start, and restart the Management application services. Stopping and restarting the Management application services causes clients connected to the server to lose connection, and they must re-log in to the server.

Monitoring and managing Management application services

To monitor the status of the Management application services, complete the following steps.

1. Launch the Server Console.
2. Click the **Services** tab (Figure 44).

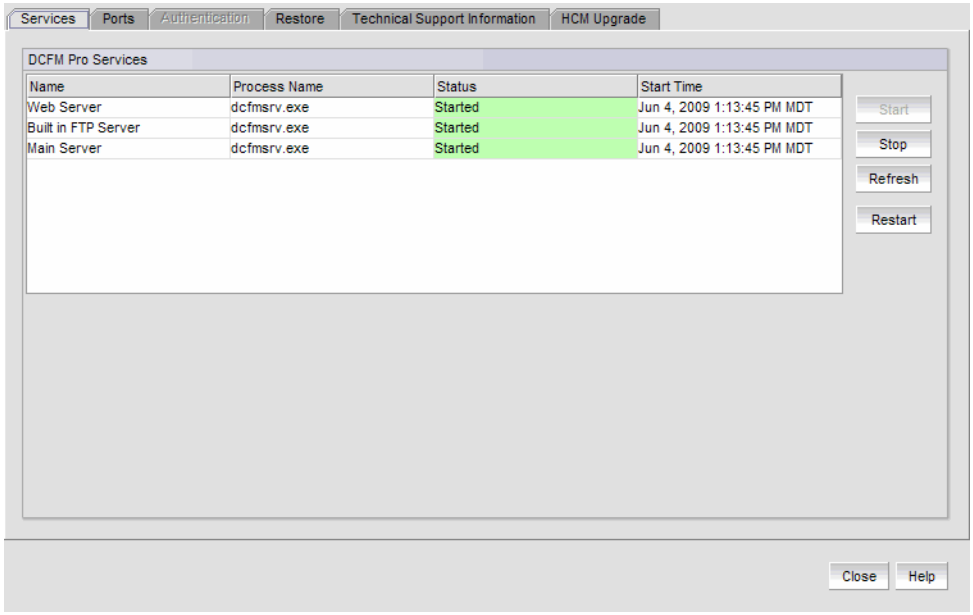


FIGURE 44 Services tab

3. Review the following information for each available service.
   - **Name**—The name of the server; for example, FTP Server or Database Server.
   - **Process Name**—The name of the process; for example, dbsrv10.exe (Database Server).

- **Status**—The status of the service; for example, started or stopped.
- **Start Time**—The date and time the service started.

4. Click **Close** to close the Server Console.

Refreshing the server status

To refresh the server status for each of the Management application services, complete the following steps.

1. Launch the Server Console.
2. Click the **Services** tab.
3. Click **Refresh** to update the table with the latest status of the services in case the services were stopped or restarted outside of the Server Console.
4. Click **Close** to close the Server Console.

Stopping all services

To stop all services, complete the following steps.

1. Launch the Server Console.
2. Click the **Services** tab.
3. Click **Stop** to stop all services.

   Note that clicking **Restart** stops and then restarts all services.
4. Click **Close** to close the Server Console.

Starting all services

To start all services, complete the following steps.

1. Launch the Server Console.
2. Click the **Services** tab.
3. Click **Start** to start all services.

   NOTE
   If the server is configured to use an external FTP server, the Server Management Console does not attempt to start the built-in FTP service.
4. Click **Close** to close the Server Console.

Restarting all services

To stop and restart all services, complete the following steps.

1. Launch the Server Console.
2. Click the **Services** tab.
3. Click **Start** or **Stop** to start or stop all services.

   Note that clicking **Restart** stops and then restarts all services.

   NOTE
   If the server is configured to use an external FTP server, the Server Management Console does not attempt to start the built-in FTP service.

4. Click **Close** to close the Server Console.

Changing server port numbers

Use the **Ports** tab of the Server Management Console to change the Management application server and Web server port numbers. The default Web Server port number is 80. The Management application server default port number is 24600.

To change the Management application server or web server port number, complete the following steps.

1. Click the **Ports** tab.
2. Type a new port number in the *<Management_Application_Name>* **Server** or **Web Server port** field.

   Do not use port 1527.

3. Click **Apply** to save the changes.

   The server automatically restarts if you change the server port number. You must manually restart the server if you change only the web server port number.

Restoring the database

To restore application data files, you must know the path to the backup files. This path is configured from the **SAN > Options** dialog box. For more information about backup, refer to "Data backup" on page 70.

To restore the application data files, complete the following steps.

1. Click the **Services** tab.
2. Stop all services.
3. Click the **Restore** tab (Figure 45).

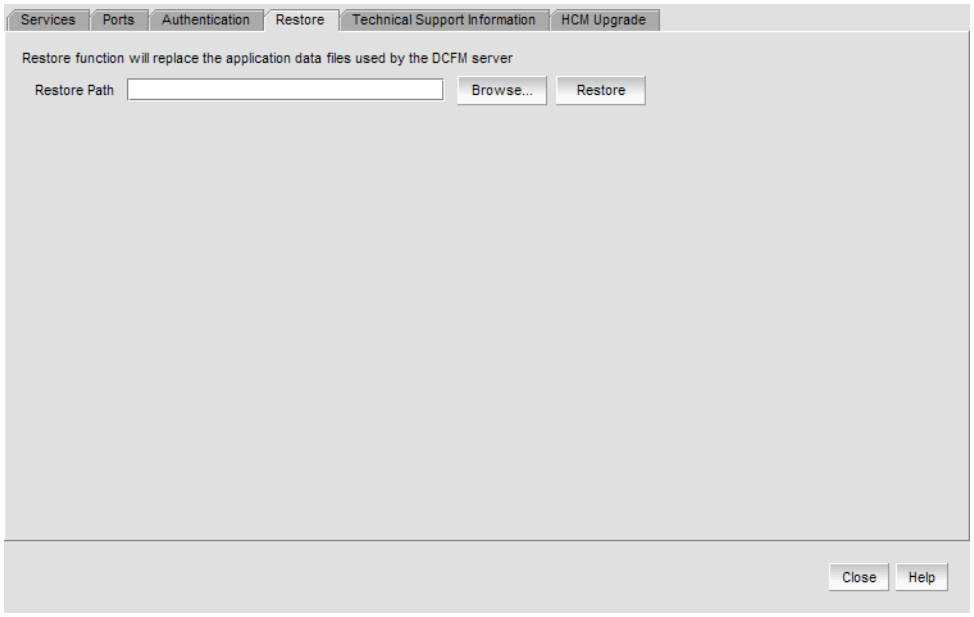


FIGURE 45 Restore tab

4. Click **Browse** to select the path (defined in the **Output Directory** field on the **Options** dialog box - **Backup** pane) to the database backup location.
5. Click **Restore**.

   Upon completion, a window displays the status of the restore operation.
6. Click the **Services** tab.
7. Click **Start** to start the server.
8. Click **Close** to close the dialog box.

Capturing technical support information

The **Technical Support Information** tab of the SMC allows you to capture technical support information for the Management application as well as the configuration files for all switches in discovered fabrics. This information is saved in a *zip* file in a location that you specify.

To capture technical support information, complete the following steps.

1. Select the **Technical Support Information** tab (Figure 46).

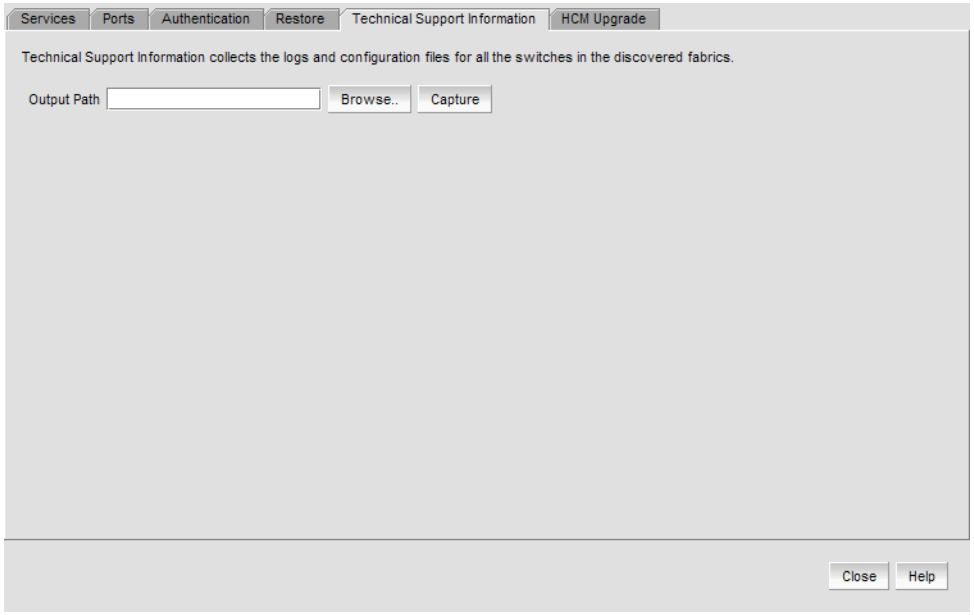


FIGURE 46 **Technical Support Information tab**

2. Click **Browse** to select the path where the **supportShow** data will be saved.

   If you do not specify an output path, the Management application automatically saves the data to the <*Install_Home*>/support directory.

3. Click **Capture**.

   A confirmation message displays when the capture is complete.

4. Click **OK**.

Upgrading HCM on the Management server

The **HCM Upgrade** tab enables you to upgrade the Management application to include a new version of HCM.

To upgrade HCM, complete the following steps.

1. Select the **HCM Upgrade** tab (Figure 47).

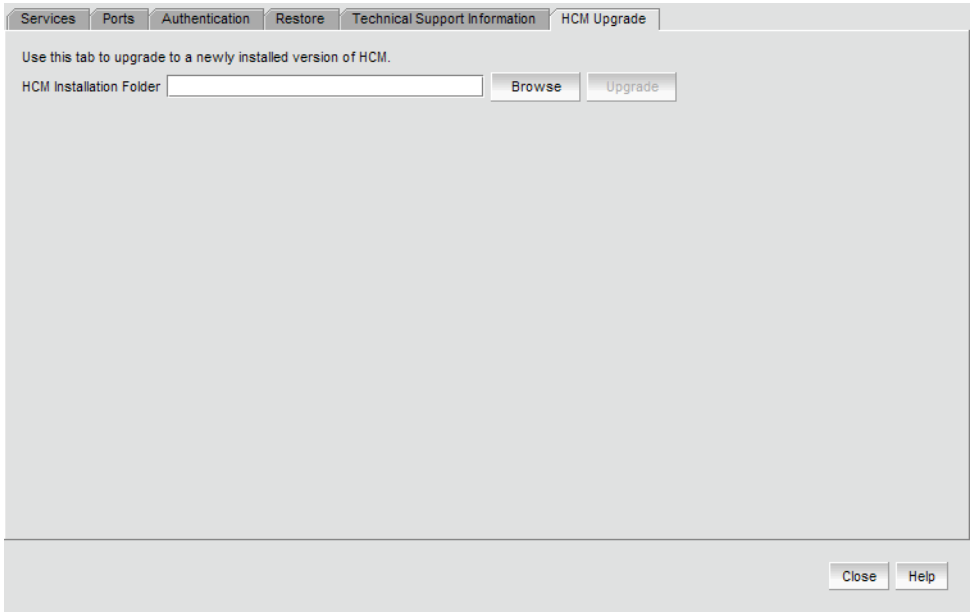


FIGURE 47 HCM Upgrade tab

2. Click **Browse** to select the HCM installation folder location (for example, C:\Program Files\BROCADE\FCHBA on Windows systems and /opt/BROCADE/FCHBA on Solaris and Linux systems).
3. Click **Upgrade**.
4. Click **Close**.

Chapter

Device Configuration 5

In this chapter

- Configuration repository management 131
- Device properties. 133
- Enhanced group management 137
- Firmware management 138
- HBA server mapping 142
- Ports 147
- Port Auto Disable 161

Configuration repository management

Configuration files are run as a Derby database as part of the Management application service; however, they are only stored as a flat file. For Windows platforms the default location is <*Install_Home*>\data\databases\<*Management_Application_Name*>db

Professional Edition only allows you to back up the configuration repository and save switch configuration. For complete feature support, you must upgrade Enterprise Edition.

For more information about the database fields, refer to "Sybase and Derby Database Fields" on page 455.

Saving switch configurations

NOTE
Save switch configuration is only supported on Fabric OS switches.

NOTE
To save switch configuration on more than one switch at a time, you must have the Enhanced Group Management license.

Configuration files are uploaded from the selected switches and stored in individual files. Files are named with the convention *cfg_fabricName_switchName_domainID*.

1. Select **Configure > FC Switch > Save**.

   The **Save Switch Configurations** dialog box is displayed (Figure 48).

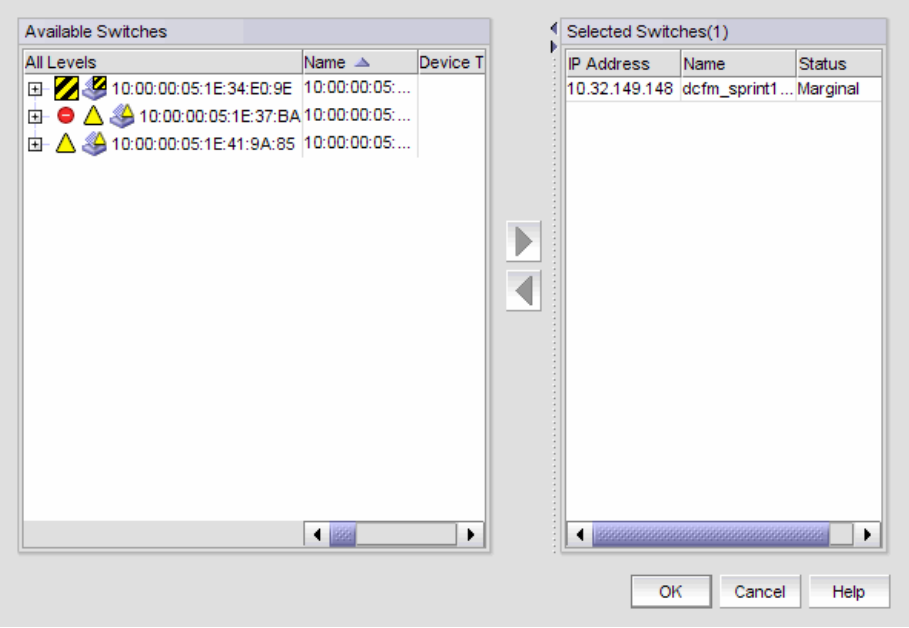


FIGURE 48 **Save switch configurations**

2. Select the switches for which you want to save configuration files from **Available Switches**.
3. Click the right arrow to move the selected switches to **Selected Switches**.
4. Click **OK**.
5. Browse to the location where you want to save the switch configuration.
6. Click **Save Configuration**.

   Configuration files from the selected switches are saved to the selected location. You can use this file to restore the saved configuration through the device's Element Manager.

Device properties

You can customize the device **Properties** dialog boxes to display only the data you need by adding, editing, and deleting property labels. You can also edit property fields to change information.

Viewing properties

To view the properties for a device or fabric, complete the following step.

Right-click any product icon and select **Properties**.

The **Properties** dialog box displays, with information related to the selected device (such as, switches, directors, HBAs, trunks, tunnels, and nodes).

Depending on the device type, any of the following port tabs may display:

- FC Ports
- GigE Ports
- IP Ports
- iSCSI Ports
- POM
- Remote Ports
- SFP
- Virtual Sessions Ports
- Virtual FCoE Ports

Depending on the device type, some of the properties listed in the following table may not be available for all products.

TABLE 19 Device property fields

Field	Description
Back to Edge Routing Support	Whether back to edge routing is supported.
Bandwidth	The bandwidth of the FCIP tunnel.
Capability	The node capability.
Compression	Whether compression is On or Off for the FCIP tunnel.
Connected Virtual FCoE Port	The fabric name, switch name, and virtual FCoE port number of the connected virtual FCoE port.
Contact	The primary contact at the customer site.
Contributors	The device contributors.
Device Type	Whether the device is an initiator or target.
Description	A description of the customer site.
Destination IP Address	The IP address of the of the FCIP tunnel destination device.
Discovery Status	The name of the device that is discovered.
Domain ID	The device's domain ID, which is the top-level addressing hierarchy of the domain.
Fabric Name	The name specified through the device Element Manager.

TABLE 19 Device property fields

Field	Description
Fastwrite	Whether fastwrite is On or Off for the FCIP tunnel.
FC Port	The FC port of the FCIP tunnel.
FCoE Capable	Whether the device is Fibre Channel over Ethernet capable.
FCS Role	Whether FCS is supported.
Firmware	The firmware version.
GigE Port	The GigE port of the FCIP tunnel.
Host Name	The host name.
IKE Policy #	The IKE policy number. Also includes the following information: • Authentication Algorithm • Encryption Algorithm • Diffie-Hellman • SA Life
IP Address	The device's IP address.
IPSec Policy #	The IPSec policy number. Also includes the following information: • Authentication Algorithm • Encryption Algorithm • SA Life
L2 Capable	Whether the device is Layer 2 capable.
L3 Capable	Whether the device is Layer 3 capable.
Location	The customer site location.
MAC	The Media Access Control address assigned to network adapters or network interface cards (NICs).
Managed By	The management program used to manage the fabric.
Master Port	The master port of the trunk.
Member Ports	The member ports of the trunk.
Model	The model number of the device.
Node Name	The name of the node.
Node WWN	The world wide name of the node.
Physical/Logical	Whether the device is a physical device or a logical device.
Port Count	The number of ports.
Port Type	The port type.
Preshared key configured	Whether the preshared key is configured for the FCIP tunnel.
Reason	The device status.
Remote Switch Name	The remote switch name of the trunk.
Remote Switch IP	The remote switch IP address of the trunk.
Remote Switch WWN	The remote switch world wide name of the trunk.
Remote Slot #	The remote slot number of the trunk.
Remote Master Port	The remote master port of the trunk.

TABLE 19 Device property fields

Field	Description
Remote Member Ports	The remote member port of the trunk.
Serial #	The hardware serial number.
Slot #	The slot number of the trunk.
Source IP Address	The IP address of the of the FCIP tunnel source device.
Speed (Gb/s)	The speed in gigabytes per second.
State	The device's state, for example, online or offline.
Status	The operational status.
Switch Name	The switch name.
Switch IP	The switch IP address.
Switch WWN	The switch world wide name.
Tape Pipelining	Whether tape pipelining is On or Off for the FCIP tunnel.
Tunnel ID	The tunnel identifier.
Type	The device type.
Unit Type	The unit type of the node.
Vendor	The product vendor.
VLAN #	The VLAN number of the FCIP tunnel.
VLAN Class of Service for Control Connection	The VLAN class of service for the control connection of the FCIP tunnel.
VLAN Class of Service for Data Connection	The VLAN class of service for the data connection of the FCIP tunnel.
WWN	The world wide name of the device.

Adding a property label

You can add a new field to any of the tabs on the **Properties** dialog box. To add a new field, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.

2. Select the tab to which you want to add a property.
3. Right-click on any label.

   The new property label displays above the one you select.

4. Select **Add**.

   The **Add Property** dialog box displays.

5. Type a label and description for the property.
6. Select the property type from the **Type** list, if available.
7. Click **OK**.

   The new property displays above the one you selected.

Editing a property label

You can edit any label that you create on the **Properties** dialog box.

To edit any field you create, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.

2. Select the tab on which you want to edit a property.
3. Right-click the label for the property you want to edit.
4. Select **Edit**.

   The **Edit Property** dialog box displays.

5. Change the label and description for the property, as needed.
6. Change the property type from the **Type** list, if available.
7. Click **OK**.

Deleting a property label

You can delete any label that you created on any of the tabs from the **Properties** dialog box. To delete a label, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.

2. Select the tab on which you want to delete a property.
3. Right-click the label for the property you want to delete.
4. Select **Delete**.
5. Click **Yes** on the confirmation message.

   The property you selected is deleted.

Editing a property field

You can edit fields on the **Properties** dialog box. To edit a field, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.

2. Select the tab on which you want to edit a field.

   Fields containing a green triangle ( ) in the lower right corner are editable.

3. Click in an editable field and change the information.
4. Click **OK**.

Enhanced group management

Use Enhanced Group Management (EGM), a separate licensed feature, to control access to specific features on Fabric OS devices. The features affected include the following:

- Firmware Download - enables you to perform group firmware download.

  For specific instructions for firmware download, refer to "Firmware management" on page 138.

- Security - enables you to perform Group Security Policy Replication.

  For specific instructions for security, refer to "Configuration repository management" on page 131.

Firmware management

A firmware file repository (Windows systems only) is maintained on the server in the following location: C:\Program Files\<*install_dir*>\data\ftproot\6.1.1\n.n.n\n.n.n\

The firmware repository is used by the internal FTP server that is delivered with the Management application software, and may be used by an external FTP server if it is installed on the same platform as the Management application software. The repository is not available to FTP servers on external platforms. The repository is used only for Fabric OS firmware. M-EOS firmware is handled through the Element Manager specific to the switch or director model.

NOTE
Non-disruptive firmware download (HCL) is not supported when downgrading from Fabric OS version 6.2 to 6.1. You must remove all non-default logical switches and disable Virtual Fabrics before downgrading.

NOTE
You cannot use Fabric OS firmware download with command line options in the Management application.

Displaying the firmware repository

The firmware repository is available on the **Firmware Management** dialog box. The Management application supports .zip and .gz compression file types for firmware files.

1. Select **Configure > Firmware Management**.

   The **Firmware Management** dialog box is displayed.

2. Select the **Repository** tab (Figure 49).

   Initially, the repository is empty. You must import firmware files into the repository. Imported firmware files are then displayed under **Firmware Repository**.

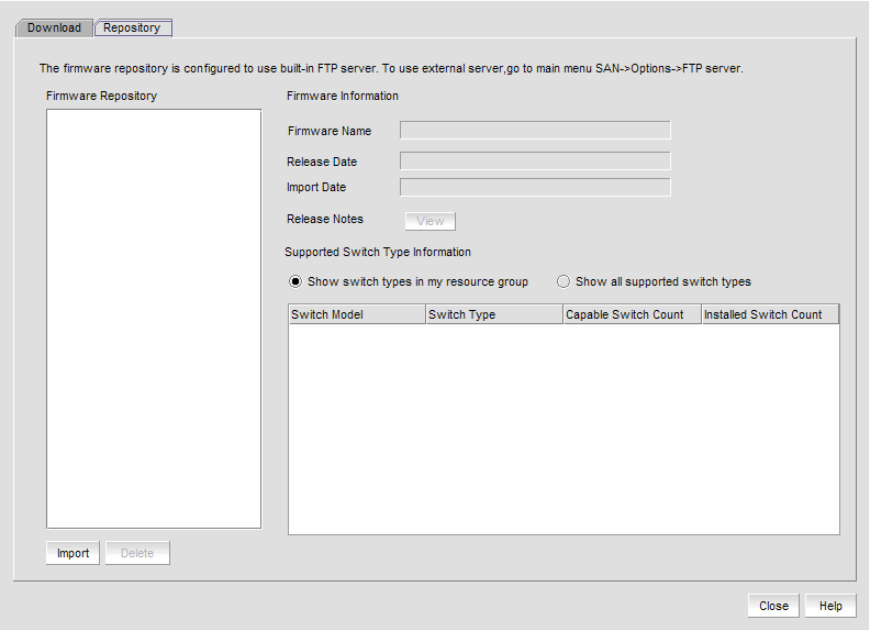


FIGURE 49 Firmware repository

3. View information about a specific firmware file by selecting the firmware file in the **Firmware Repository**.

   The **Firmware Name**, **Release Date**, and **Import Date** are displayed. You may also view the **Release Notes**, if the release notes were imported.

Importing a firmware file and release notes

Firmware files and release notes can be imported into the Firmware Repository.

1. Select **Configure > Firmware Management**.

   The **Firmware Management** dialog box is displayed.

2. Select the **Repository** tab (Figure 49).

3. Click **Import**.

   The **Import Firmware from File** dialog box is displayed (Figure 50).

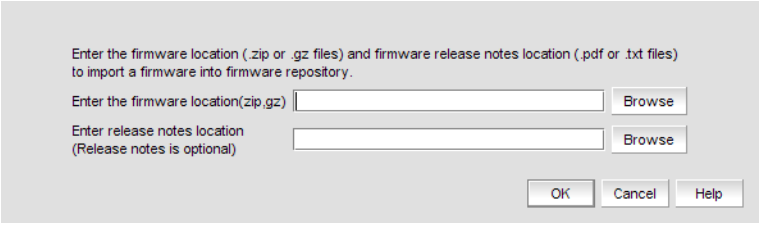

Enter the firmware location (.zip or .gz files) and firmware release notes location (.pdf or .txt files)
to import a firmware into firmware repository.
Enter the firmware location(zip,gz)
Browse
Enter release notes location
(Release notes is optional)
Browse
OK
Cancel
Help

FIGURE 50 Import firmware

4. Type in the location of the firmware file and release notes, or use **Browse** to select the location.

   The Management application supports .zip and .gz compression file types for firmware files.

5. Click **OK**.

   You return to the **Repository** tab. The file is listed in the Firmware Repository when the import is complete and successful.

Deleting a firmware file

Firmware files can be deleted from the Firmware Repository.

1. Select **Configure > Firmware Management**.

   The **Firmware Management** dialog box is displayed.

2. Select the **Repository** tab (Figure 49).

3. Select one or more firmware files from the Firmware Repository for deletion.

4. Click **Delete**.

   A confirmation dialog displays. Click **Yes** to confirm. The firmware file is deleted from the repository.

Downloading firmware

NOTE
Non-disruptive firmware download (HCL) is not supported when downgrading from Fabric OS version 6.2 to 6.1. You must remove all non-default logical switches and disable Virtual Fabrics before downgrading.

NOTE
You cannot use Fabric OS firmware download with command line options in the Management application.

You can download firmware using the **Firmware Management** dialog box.

1. Select **Configure > Firmware Management**.

   The **Firmware Management** dialog box is displayed.

2. Select the **Download** tab (Figure 51).

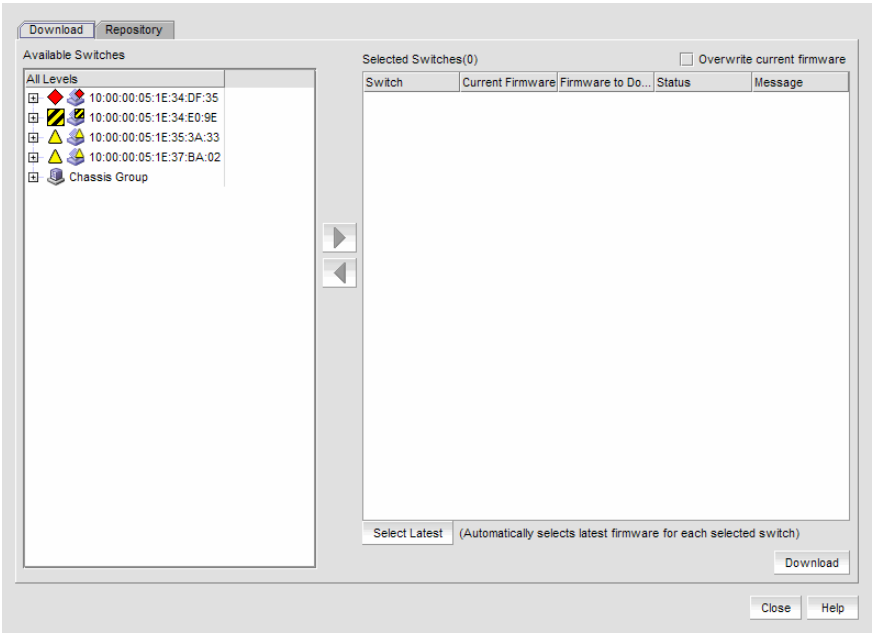


FIGURE 51 **Firmware download**

3. Select one or more switches from **Available Switches**.
4. Click the right arrow to move the switches to **Selected Switches**.
5. Select a specific version from the **Firmware to Download** column, or use **Select Latest** to automatically select the latest version.

   If you have your FTP or SCP Server configured to use an external FTP or SCP Server, the **Firmware to Download** column is empty.

6. If you want to overwrite the current firmware, even if the selected version is the same as the version currently running on the switch, click the **Overwrite Current Firmwares** check box.

7. If you configured an external server (in the **Options** dialog box), choose from one of the following options:
   - Select **External FTP Server** to download from the external FTP server.
   - Select **SCP Server** to download from the external SCP server.
8. Enter the path to the firmware directory (only displays if external server is configured in **Options** dialog box).
9. Click **Download**.

   While the firmware is downloaded to the device, the **Status** column displays the current download status. Once firmware download is complete, the **Message** column displays whether the download was a success or failure.

HBA server mapping

HBAs and servers discovered through a fabric can be easily identified in the topology by their product icons. For a list of products and their icons, refer to "Product icons" on page 16. Once identified in the topology, you can create servers and assign the HBAs to them and import an externally created HBA server mapping file (.CSV) to the Management application.

NOTE
The Management application now enables you to map HBAs from multiple fabrics (previous versions limited HBA mapping to one fabric).

The Management application also enables you to discover hosts directly using Host discovery (for step-by-step instructions, refer to "Host discovery" on page 44). If you discover a host directly, when you open the **HBA Server Mapping** dialog box the Management application automatically groups all HBAs under the host.

If you create a new HBA server and associate HBAs to it, then you try to discover a host with the same HBAs using Host discovery, the HBA's discovered using host discovery must match the HBAs associated to the HBA server exactly; otherwise, Host discovery will fail.

Creating a new HBA server

To create a new server, complete the following steps.

1. Right-click an HBA icon and select **Server Port Mapping**.

   The **HBA Server Mapping** dialog box displays.

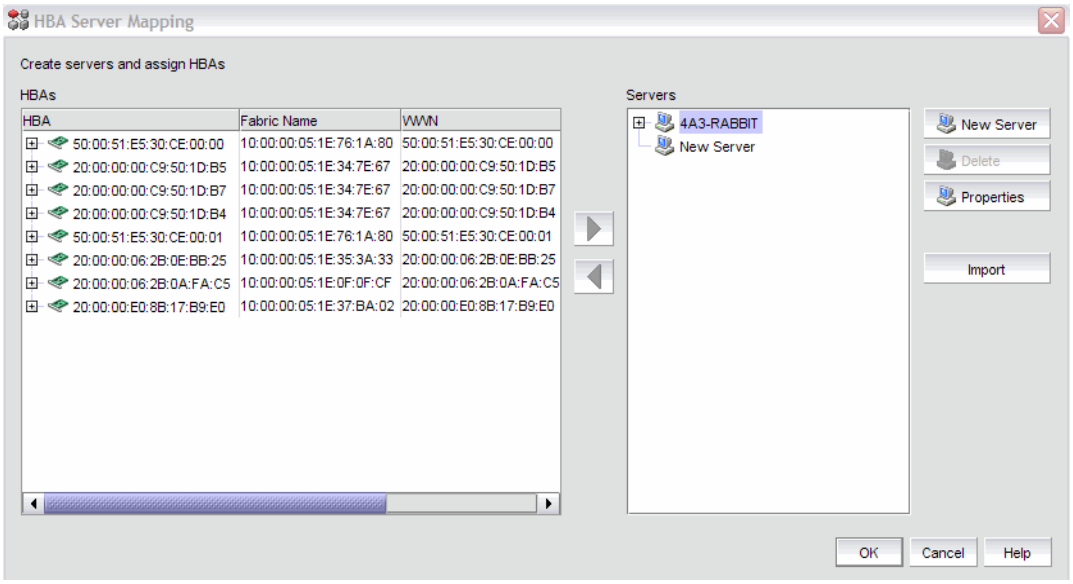


FIGURE 52 **HBA Server Mapping Dialog Box**

2. Click **New Server**.

   A new server displays in the **Servers** table in edit mode.

3. Double-click the new server name to make it editable, type a name for the new Server, and press **Enter**.

   The name of the new server appears in the **Servers** table in alphabetical order. To assign HBAs to this server, refer to "Associating an HBA with an HBA server" on page 144.

4. Click **OK** to save your changes and close the **HBA Server Mapping** dialog box.

Renaming an HBA server

To rename a server, complete the following steps.

1. Right-click an HBA icon and select **Server Port Mapping**.

   The **HBA Server Mapping** dialog box displays.

2. Click the server you want to rename in the **Servers** table, wait a moment, and then click it again.

   The server displays in edit mode.

3. Type a new name for the server.

   The name of the server appears in the **Servers** table in alphabetical order with the new name. To assign HBAs to this server, refer to "Associating an HBA with an HBA server" on page 144.

4. Click **OK** to save your changes and close the **HBA Server Mapping** dialog box.

Deleting an HBA server

To delete a server, complete the following steps.

1. Right-click an HBA icon and select **Server Port Mapping**.

   The **HBA Server Mapping** dialog box displays.

2. Select the Server you want to delete in the **Servers** table.

3. Click **Delete**.

   The selected Server is deleted. Any HBAs associated with the Server are automatically moved from the **Servers** table to the **HBAs** table.

4. Click **OK** to save your changes and close the **HBA Server Mapping** dialog box.

Viewing Server properties

To view Server properties, complete the following steps.

1. Right-click an HBA icon and select **Server Port Mapping**.

   The **HBA Server Mapping** dialog box displays.

2. Select the HBA Server port you want to view in the **Servers** table.

3. Click **Properties**.

   The **Properties** dialog box for the selected port displays.

4. Click **OK** to close the **Properties** dialog box.

5. Click **OK** to close the **HBA Server Mapping** dialog box.

Associating an HBA with an HBA server

ATTENTION
Discovered information overwrites your user settings.

To associate an HBA with a server, complete the following steps.

1. Right-click an HBA icon and select **Server Port Mapping**.

   The **HBA Server Mapping** dialog box displays.

2. Select the server to which you want to assign HBAs in the **Servers** table.

3. Select the HBA from the **HBAs** table on the left and click the right arrow.

   The HBA displays in the **Servers** table. The HBA is now associated with the selected server.

4. Click **OK** to save your changes and close the **HBA Server Mapping** dialog box.

   On the Connectivity Map, the HBA displays in the server.

Importing HBA-to-server mapping

The **HBA Server Mapping** dialog box enables you to import externally created HBA-to-Server mapping information into the application. The imported file must be in CSV format. The first row must contain the headers (wwn, name) for the file.

Example

```
wwn,name
20:00:00:00:C9:69:D5:27, s1
20:00:00:05:1E:0A:35:0E, s2
```

When the import is complete a result summary displays with the information listed in Table 20.

TABLE 20 Import Results

Value	Definition
Total Valid Input Records	Number of lines identified in the CSV file without any errors (excluding the Header).
Unique HBA WWNs Recognized	Number of unique HBAs identified in the CSV file.
Servers Created or Identified	Number of HBAs identified in the CSV file already discovered, and which are either online or offline but not deleted.
Conflicting HBA Mappings	Number of occurrences where you were asked to decide whether to override previously discovered information. If you select Yes to All, or No to All, each occurrence where conflict resolution occurs automatically is counted as one conflict.
Overwritten HBA Mappings	Number of times a previously discovered mapping is overwritten during the import process.
Importing Errors	Number of errors encountered during the import.
Details	Tabulates the error information with respect to the line number where it occurred.

To import HBA server mapping, complete the following steps.

1. Right-click an HBA icon and select **Server Port Mapping**.

   The **HBA Server Mapping** dialog box displays.

2. Click **Import**.

   The **Import** dialog box displays.

3. Browse to the file (CSV format only) you want to import.

4. Click **Open** on the **Import** dialog box.

   The file imports, reads, and applies all changes line-by-line and performs the following:

   - Checks for correct file structure and well-formed WWNs, and counts number of errors.

     If more than 5 errors occur, import automatically cancels. Edit the Server HBA mapping file and try again.

   - Checks for duplicate HBAs.

     If duplicates exist, a message displays with the duplicate mappings detailed. Click **Yes** to continue. Click **No** to edit the Server HBA mapping file and try again.

   - Checks for existing mappings in the current map.

     If a mapping already exists, a message displays with the current mapping information. Click **Yes** to overwrite the current mapping. Click **Yes to All** to overwrite all mapping conflicts. Click **No** to leave the current mapping. Click **No to All** to leave all current mappings when conflict occurs. Click **Cancel** to cancel the import.

5. Click **OK** to close the **Import Results** dialog box.
6. Click **OK** to close the **HBA Server Mapping** dialog box.

Removing an HBA from a HBA server

To remove an HBA from a Server, complete the following steps.

1. Right-click an HBA icon and select **Server Port Mapping**.

   The **HBA Server Mapping** dialog box displays.

2. Select the HBA from the **Servers** table on the right and click the left arrow.

   The HBA you selected is removed from the **Servers** table and the HBA is no longer associated with the server.

3. Click **OK** to save your changes and close the **HBA Server Mapping** dialog box.

   On the Connectivity Map, the HBA displays on its own.

Ports

You can enable and disable ports, as well as view port details, properties, type, status, and connectivity.

Viewing port connectivity

The connected switch and switch port information is displayed for all ports.

To view port connectivity, choose one of the following steps:

- Right-click a product icon and select **Port Connectivity**.
- Select a product icon and select **Monitor > Port Connectivity**.

  The **Port Connectivity View** dialog box displays (Figure 53).

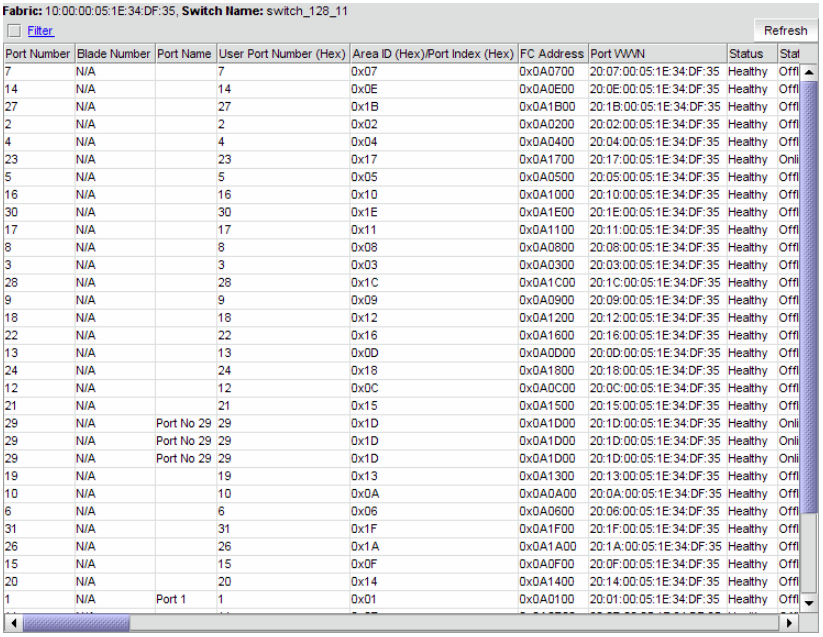

Fabric: 10:00:00:05:1E:34:DF:35, Switch Name: switch_128_11
Filter
Refresh
Port Number | Blade Number | Port Name | User Port Number (Hex) | Area ID (Hex)/Port Index (Hex) | FC Address | Port WWN | Status | Stat
7 N/A 7 0x07 0x0A0700 20:07:00:05:1E:34:DF:35 Healthy Offl
14 N/A 14 0x0E 0x0A0E00 20:0E:00:05:1E:34:DF:35 Healthy Offl
27 N/A 27 0x1B 0x0A1B00 20:1B:00:05:1E:34:DF:35 Healthy Offl
2 N/A 2 0x02 0x0A0200 20:02:00:05:1E:34:DF:35 Healthy Offl
4 N/A 4 0x04 0x0A0400 20:04:00:05:1E:34:DF:35 Healthy Offl
23 N/A 23 0x17 0x0A1700 20:17:00:05:1E:34:DF:35 Healthy Onli
5 N/A 5 0x05 0x0A0500 20:05:00:05:1E:34:DF:35 Healthy Offl
16 N/A 16 0x10 0x0A1000 20:10:00:05:1E:34:DF:35 Healthy Offl
30 N/A 30 0x1E 0x0A1E00 20:1E:00:05:1E:34:DF:35 Healthy Offl
17 N/A 17 0x11 0x0A1100 20:11:00:05:1E:34:DF:35 Healthy Offl
8 N/A 8 0x08 0x0A0800 20:08:00:05:1E:34:DF:35 Healthy Offl
3 N/A 3 0x03 0x0A0300 20:03:00:05:1E:34:DF:35 Healthy Offl
28 N/A 28 0x1C 0x0A1C00 20:1C:00:05:1E:34:DF:35 Healthy Offl
9 N/A 9 0x09 0x0A0900 20:09:00:05:1E:34:DF:35 Healthy Offl
18 N/A 18 0x12 0x0A1200 20:12:00:05:1E:34:DF:35 Healthy Offl
22 N/A 22 0x16 0x0A1600 20:16:00:05:1E:34:DF:35 Healthy Offl
13 N/A 13 0x0D 0x0A0D00 20:0D:00:05:1E:34:DF:35 Healthy Offl
24 N/A 24 0x18 0x0A1800 20:18:00:05:1E:34:DF:35 Healthy Offl
12 N/A 12 0x0C 0x0A0C00 20:0C:00:05:1E:34:DF:35 Healthy Offl
21 N/A 21 0x15 0x0A1500 20:15:00:05:1E:34:DF:35 Healthy Offl
29 N/A Port No 29 29 0x1D 0x0A1D00 20:1D:00:05:1E:34:DF:35 Healthy Onli
29 N/A Port No 29 29 0x1D 0x0A1D00 20:1D:00:05:1E:34:DF:35 Healthy Onli
29 N/A Port No 29 29 0x1D 0x0A1D00 20:1D:00:05:1E:34:DF:35 Healthy Onli
19 N/A 19 0x13 0x0A1300 20:13:00:05:1E:34:DF:35 Healthy Offl
10 N/A 10 0x0A 0x0A0A00 20:0A:00:05:1E:34:DF:35 Healthy Offl
6 N/A 6 0x06 0x0A0600 20:06:00:05:1E:34:DF:35 Healthy Offl
31 N/A 31 0x1F 0x0A1F00 20:1F:00:05:1E:34:DF:35 Healthy Offl
26 N/A 26 0x1A 0x0A1A00 20:1A:00:05:1E:34:DF:35 Healthy Offl
15 N/A 15 0x0F 0x0A0F00 20:0F:00:05:1E:34:DF:35 Healthy Offl
20 N/A 20 0x14 0x0A1400 20:14:00:05:1E:34:DF:35 Healthy Offl
1 N/A Port 1 1 0x01 0x0A0100 20:01:00:05:1E:34:DF:35 Healthy Offl

FIGURE 53 **Port Connectivity View Dialog Box**

Loop devices are displayed in multiple rows, one row for each related device port.

If no switch or device is connected to the port, then the related fields are empty.

The following table details the information located (in alphabetical order) on the **Port Connectivity View** dialog box.

TABLE 21 Port connectivity fields

Field	Description
Actual Distance	The actual distance for end-to-end port connectivity.
Area ID (Hex)	The area ID (in hexadecimal) of the port.
Blade Number	The number of the blade.
Blocked	Whether the selected port is blocked.

TABLE 21 Port connectivity fields

Field	Description
Buffer Limited	Whether buffers are limited.
Buffers Needed/Allocated	The ratio of buffers needed relative to the number of buffers allocated.
Calculated Status	The operational status. There are four possible operation status values: • Up - Operation is normal. • Down - The port is down or the route to the remote destination is disabled. • Disabled - The connection has been manually disabled. • Backup Active - The backup TCP port is active due to a failover.
Capability	The device capability of the connected device port. The value is mapped depending on whether it is a name server (NS) or a FICON device.
Connected Blade Number	The number of the connected blade.
Connected Port Area ID (Hex) Port Index (Hex)	The area ID and the port index (both in hexadecimal) of the connected port.
Connected Port Name	The name of the connected port.
Connected Port Number	The number of the connected port.
Connected Port Speed	The speed of the connected port.
Connected Port Status	The connection status. There are four possible operation status values: • Up - Operation is normal. • Down - The port is down or the route to the remote destination is disabled. • Disabled - The connection has been manually disabled. • Backup Active - The backup TCP port is active due to a failover.
Connected Port State	The connected port's state; for example, online or offline.
Connected Port WWN	The world wide name of the connected port.
Connected User Port Number (Hex)	The port number (in hexadecimal) of the connected user port.
COS	The class of service (CoS) value, which ranges between zero (low priority) and seven (high priority).
Device Node WWN	The world wide name of the device node.
Device Symbolic Name	The symbolic name of the device node.
Device Port/Switch Domain ID	The device port and switch domain ID.
Device Port/Switch WWN	The device port and switch world wide name.
Device Port/Switch Name	The device port and switch name.
Device Port/Switch State	The device port and switch state.
Device Port/Switch Manufacturer	The device port and manufacturer of the switch.
Device Port/Switch Manufacturing Plant	The device port and switch manufacturing plant.
Device Port / Switch Type Number	The device port and switch type number.

TABLE 21 Port connectivity fields

Field	Description
Device Type	The device type; for example, target or initiator.
FC4 Type	The active FC4 type; for example, SCSI.
FC Address	The Fibre Channel address. Each FC port has both an address identifier and a world wide name (WWN).
Flag	Whether a flag is on or off.
Hard Address	The hard address of the device.
Host Name	The name of the host.
Long Distance	Whether the connection is considered to be normal or longer distance.
Model	The model name and number of the device.
Parameter	Device parameters.
Physical/Virtual/NPIV	Whether the port is a physical port, a virtual port, or an NPIV_port.
Port Address	The port's address.
Port IP Address	The port's IP address.
Port Module	The port's module.
Port Name	The port's name.
Port Number	The port's number.
Port Type	The type of port; for example, U_Port (universal port) or FL_Port (Fabric loop port).
Port WWN	The world wide name of the port.
Prohibited	Whether the allow/prohibit matrix is activated.
Serial #	The port's serial number.
Speed	The current port speed, in gigabits per second.
State	The port's state; for example, online or offline.
Switch Dynamic Load Sharing	Whether switch dynamic load sharing is enabled.
Switch FCS Role	Whether the Fabric Configuration Server (FCS), which is the primary point of control that manages all the switches within a fabric, is enabled.
Switch FMS mode	Whether the File Management Solution (FMS) mode is enabled.
Switch Has Certificate	Whether the switch has a certificate (true or false).
Switch IDID	Whether the switch's insistent domain ID (IDID) is enabled. If it is enabled, the IDID is the same ID that is requested during switch reboots, power cycles, CP failovers, firmware downloads, and fabric reconfiguration.
Switch in Order Delivery	Whether switch in-order delivery is enabled.
Switch IP	The switch's IP address.
Switch Port Count	The number of ports on the switch.
Switch Role	The role of the switch; for example, subordinate.

TABLE 21 Port connectivity fields

Field	Description
Switch Routing Policy	Whether a routing policy, for example, port-based routing policy, is enabled.
Switch Secure Mode	Whether switch secure mode is enabled.
Switch Status	The operational status. There are four possible operation status values: • Up - Operation is normal. • Down - The port is down or the route to the remote destination is disabled. • Disabled - The connection has been manually disabled. • Backup Active - The backup TCP port is active due to a failover.
Switch Supplier Serial Number	The serial number of the switch supplier.
Switch Version	The switch's version number.
Tag	The tag number of the port.
Unit Type	The switch unit type.
User Port Number	The port number of the user's device.
Vendor	The hardware vendor's name.

Refreshing the port connectivity view

To obtain configuration changes that occurred since the **Port Connectivity View** dialog box opened, click **Refresh**.

Enabling a port

To enable a port from the port connectivity view, right-click the port you want to enable from the **Port Connectivity View** dialog box and select **Disable/Enable Port > Enable**.

Disabling a port

To disable a port from the port connectivity view, right-click the port you want to disable from the **Port Connectivity View** dialog box and select **Disable/Enable Port > Disable**.

Filtering port connectivity

To filter results from the port connectivity view, complete the following steps.

1. Click the **Filter** link from the **Port Connectivity View** dialog box

   The **Filter** dialog box displays (Figure 54).

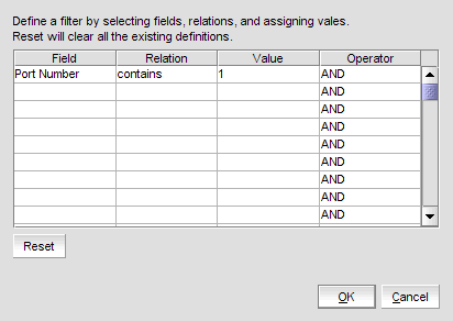


FIGURE 54 Filter Dialog Box

2. Click a blank cell in the **Field** column to select the property from which to filter the results.
3. Click a blank cell in the **Relation** column to select an action operation.

   The following actions are available:

   - ==
   - !=
   - <
   - >
   - <=
   - >=
   - contains
   - matches
4. Define a filter by entering a value that corresponds to the selected property in the **Value** column.
5. Repeat steps 2 through 4 as needed to define more filters.
6. Click **OK**.

   The **Port Connectivity View** dialog box displays. If filtering is already enabled, only those ports that meet the filter requirements display. To enable the filter, select the **Filter** check box.

Resetting the filter

Reset immediately clears all existing definitions. You cannot cancel the reset.

To reset the **Filter** dialog box, complete the following steps.

1. Click the **Filter** link from the **Port Connectivity View** dialog box.

   The **Filter** dialog box displays.

2. Click **Reset**.

   All existing definitions are cleared automatically. You cannot cancel the reset.

Enabling the filter

To enable the filter, select the **Filter** check box.

Disabling the filter

To disable the filter, clear the **Filter** check box.

Viewing port details

To view port details, complete the following steps.

1. Right-click the port for which you want to view more detailed information on the **Port Connectivity View** dialog box and select **Show Details**.

   The **Port Details** dialog box displays(Figure 53).

COLUMN	VALUE
Actual Distance	
Area ID (Hex)/Port Index (Hex)	20
Blade Number	N/A
Blocked	
Buffer Limited	N/A
Buffers Needed/Allocated	
COS	
Capability	
Connected Blade Number	N/A
Connected Port Area ID (Hex)/Port Index (Hex)	0 (0x00)
Connected Port Name	
Connected Port Number	0
Connected Port Speed	
Connected Port State	
Connected Port Status	
Connected Port WWN	
Connected User Port Number (Hex)	
Device Node WWN	
Device Port / Switch Domain Id	
Device Port / Switch Manufacturer	
Device Port / Switch Manufaturing Plant	
Device Port / Switch Name	
Device Port / Switch State	
Device Port / Switch Type Number	
Device Port / Switch WWN	

FIGURE 55 Port Details dialog box

2. Review the port information.

   For the list of fields on the **Port Details** dialog box, refer to Table 21 on page 147.

3. Sort the results by clicking on the column header.
4. Rearrange the columns by dragging and dropping the column header.
5. Click the close (X) button to close this dialog box.

Viewing ports and port properties

To view ports on the Connectivity Map, right-click a product icon and select **Show Ports**.

NOTE
Show Ports is unavailable when the map display layout is set to **Free Form** (default).

NOTE
This feature is only available for connected products. On bridges and CNT products, only utilized Fibre Channel ports display; IP ports do not display.

To view a port's properties, right-click on a port and select **Properties**, or double-click on the port.

The port **Properties** dialog box displays (Figure 53).

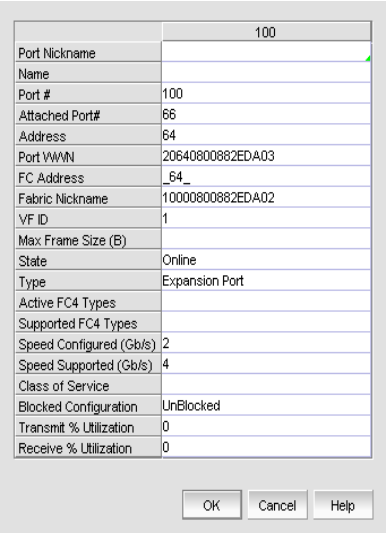


FIGURE 56 Port Properties Dialog Box

The following port types are available depending on the selected device:

- FC Ports
- GigE Ports
- IP Ports
- iSCSI Ports

  NOTE
  iSCSI ports that have an FC Address of all zeros are inactive. All others are active.

- Virtual Sessions Ports
- Virtual FCoE Ports

Depending on the port type, some of the following properties (Table 22) may not be available for all products.

TABLE 22 Port property fields

Field	Description
# Virtual Session Ports	The number of virtual session ports associated with the GE port.
Additional Port Info	Additional error information relating to the selected port.
Address	The address of the port.
Active FC4 Types	The active FC4 types.
Active Tunnels	The number of active tunnels.
Area ID (hex)/Port Index (hex)	The area identifier, in hexadecimal, of the switch-to-product connection.
Associated GE Port	The port number of the associated GE port.
Attached Port #	The port number of the attached product.
Blocked	The configuration of the switch (blocked or unblocked).
Buffers Desired	The number of buffers desired but not allocated.
Buffers Allocated	The number of buffers allocated.
Class	The class of the port.
Class of Service	The class of service.
Connected Devices	The number of connected devices. Click the icon in the right side of the field to open the **Virtual FCoE Port <Number> Connected Devices** dialog box.
Connected Switch	The name of the connected switch.
Delete button	Click to delete.
Device Type	Whether the device is an initiator or target.
Distance Actual (km)	The actual distance (in km) for end-to-end port connectivity.
Distance Estimated (km)	The estimated distance (in km) for end-to-end port connectivity.
Fabric	The fabric's IP address.
Fabric Name	The name of the fabric.
FCIP Capable	Whether the port is FCIP capable.
FC Port Count	The number of FC ports on the device.
Flag (FICON related)	Whether a flag is on or off.
GigE Port Count	The number of GigE ports on the device.
Inband Management Status	The inband management status (online or offline).
Index	The index of the Virtual FCoE Port.
Interface Count	The interface count.
iSCSI button	Click to launch the Element Manager.
iSCSI Capable	Whether the port is iSCSI capable or not.
Locked Port Type	The port type of the locked product.
Long Distance Setting	Whether the connection is considered to be normal or longer distance.

TABLE 22 Port property fields

Field	Description
MAC Address	The Media Access Control address assigned to a network adapters or network interface cards (NICs).
Manufacturer Plant	The name of the manufacturer plant.
Modify button	Click to launch the Element Manager.
Model	The model number of the device.
Name	The name of the switch.
Performance list	Select to launch the dialog box of one of the following performance options: • Real Time Graph • HIstorical Graph • HIstorical Report
Physical/Logical	Whether the port is a physical port or a logical port.
Port Address	The address of the port.
Port #	The number of the port.
Port ID	The identifier of the port.
Port Module	The port's module.
Port NPIV	Number of NPIV ports.
Port Speed (Gb/s)	The port speed, in Gbits per second.
Port State	The port state (online or offline).
Port Status	The port's operational status (online or offline).
Port WWN	The port's world wide name.
Prohibited	Whether the port is prohibited.
Protocol	The network protocol, for example, Fibre Channel.
Serial #	The hardware serial number.
Slot #	The location (slot) of the port.
Speed (Gb/s)	The port speed, in Gbits per second.
State	The port state (online or offline).
Status	The port's operational status (online or offline).
Switch	The name of the switch.
Symbolic Name	The symbolic name of the port.
Tag	The tag number of the port.
Troubleshooting list	Select to launch the dialog box of one of the following troubleshooting options: • IP Ping • IP Traceroute • IP Performance
Type	The type of port, for example, U_port.
Tunnel Count	The number of tunnels.
User Port #	The number of the user port.

TABLE 22 Port property fields

Field	Description
Vendor	The product vendor.
Virtual FCoE Port Count	The number of FC ports on the device.

Port types

On the Connectivity Map, right-click a switch icon and select **Show Ports**. The port types display showing which ports are connected to which products.

NOTE
Show Ports is unavailable when the map display layout is set to **Free Form**.

NOTE
This feature is only available for connected products. On bridges and CNT products, only utilized Fibre Channel ports display. IP ports do not display.

TABLE 23 Port types

Port Type	Description
E	An expansion port connecting two Fibre Channel switches.
EX	On a Fibre Channel Router, a connection between a fibre channel router and a fibre channel switch
F	On a Fibre Channel switch, a port that supports an N_Port.
FL	An N_port or F_port that supports arbitrated loop functions associated with arbitrated loop topology.
VE	A virtual E_port configured for an FCIP Tunnel.
VEX	A virtual EX_port configured in an FCIP Tunnel.

Showing connected ports

You can jump from a port to its connected port.

1. Right-click the product whose port connection you want to determine and select **Show Ports**.

   The product's ports display.

2. Right-click a port and select **Connected Port**.

   The focus jumps to the connected port and the connection is highlighted.

Viewing port connection properties

You can view the information about products and ports on both sides of the connection.

1. Right-click the connection between two end devices on the Connectivity Map and select **Properties**.

   OR

   Double-click the connection between two devices on the Connectivity Map.

   The **Connection Properties** dialog box displays.

   NOTE
   If one of the devices is in an unknown state, the Product 1 and Product 2 information displays; however, the **Connections** table information does not display.

2. Review the following information:

   - Product properties for both devices.
   - Connection properties.
   - Selected connection port properties.

   Depending on the device type at either end of the connection, some of the following fields (Table 24) may not be available for all products.

TABLE 24 Connection property fields

Field	Description
Product Properties table	The product information for the two connected switches.
Domain ID	The domain ID of the selected switch and product in xxs(yy) format, where *xx* is the normalized value and *yy* is the actual value.
Fabric Name	The world wide name of the fabric.
IP Address	The IP address of the switch.
Switch Name	The name of the switch.
WWN	The world wide name of the switch.
Connections table	
1-Port #	The port number of the first switch.
1-Port Type	The port type of the first switch.
1-WWPN	The world wide port number of the first switch.
1-MAC Address	The MAC address of the first switch.
1-IP Address	The IP address of the first switch.
1-Trunk	Whether there is a trunk on the first switch.
1-Speed (Gbps)	The speed of the first switch.
2-Port #	The port number of the second switch.
2-Port Type	The port type of the second switch.
2-WWPN	The world wide port number of the second switch.
2-MAC Address	The MAC address of the second switch.

TABLE 24 Connection property fields

Field	Description
2-IP Address	The IP address of the second switch.
2-Trunk	Whether there is a trunk on the second switch.
2-Speed (Gbps)	The speed of the second switch.
Selected Connection Properties table	The connected device port information.
Name	The name of the switch.
Slot #	The slot number of the switch.
User Port #	The user port number of the switch.
Area ID (hex)/Port Index (hex)	The area identifier, in hexadecimal, of the switch-to-product connection.
Port Address	The address of the port.
GE Port #	The GE port number of the switch.
MAC Address	The MAC address of the switch.
Status	The operational status of the switch
State	The operational status of the port.
Port Module	The port's module.
Protocol	The network protocol, for example, Fibre Channel.
Buffers Desired	The number of buffers required but not allocated.
Buffers Allocated	The number of buffers allocated.
Distance Actual (km)	The actual distance (in km) for end-to-end port connectivity.
Distance Estimated (km)	The estimated distance (in km) for end-to-end port connectivity.
Long Distance Setting	Whether the connection is considered to be normal or longer distance.
Physical/Logical	Whether the port is a physical port or a logical port.
Locked Port Type	The port type of the locked product.
Port NPIV	The number of NPIV ports.
Connected Switch	The name of the connected switch.
Blocked	The configuration of the switch (blocked or unblocked).
Prohibited	Whether the port is prohibited.

3. Click **Close** to close the dialog box.

Determining inactive iSCSI devices

For router-discovered iSCSI devices, you can view all of the inactive iSCSI devices in one list. To do this, use the **Ports Only** view and then sort the devices by FC Address. The devices that have an FC address of all zeros are inactive.

1. Select **View All**, **Levels**, and then **Ports Only** from the main window.
2. Use the scroll bar to view the columns to the right and locate the **FC Address** column in the **Ports Only** list.
3. Click the column label to sort the column in ascending order, if needed.

   iSCSI ports that have an FC Address of all zeros are inactive. All others are active.

Determining port status

You can determine whether a port is online or offline by looking at the Connectivity Map or the Product List. On the Connectivity Map, right-click on the product whose ports you want to view and select **Show Ports**.

To determine a port's status through the Product List, scroll down the Product List to the product whose ports you want to see and click the added icon ( ).

Viewing port optics

To view port optics, complete the following steps.

1. Right-click the switch for which you want to view port optic information on the Connectivity Map and select **Port Optics (SFP)**.

   The **Port Optics (SFP)** dialog box displays(Figure 57).

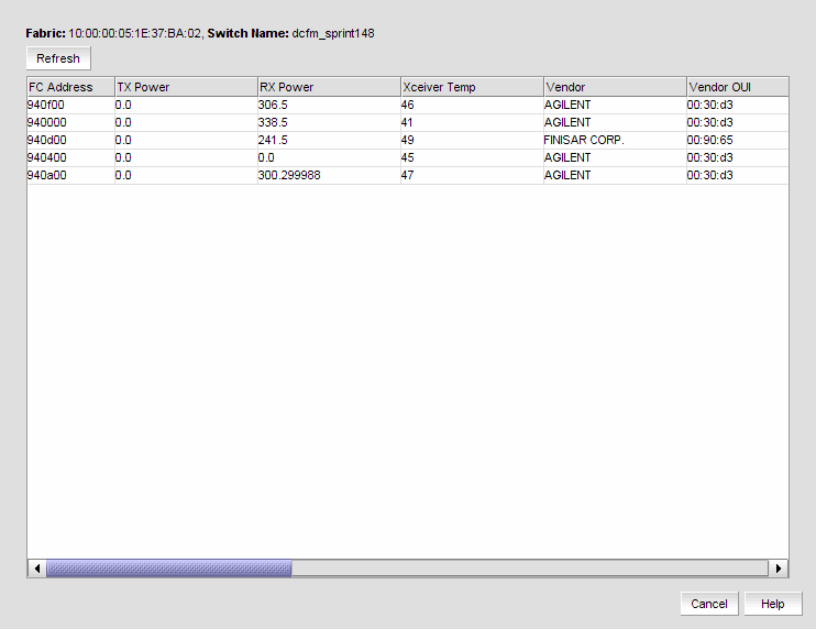


FIGURE 57 Port Optics Dialog Box

2. Review the port optics information.
    - **Slot/Port #**—The slot and port number of the selected fabric.
    - **FC Address**—The Fibre Channel address of the port.
    - **TX Power**—The power transmitted to the SFP in dBm and uWatts.

      NOTE
      The uWatts display requires devices with Fabric OS 6.1.0 and later. Devices running Fabric OS 6.0.0 and earlier only display dBm.

    - **RX Power**—The power received from the port in dBm and uWatts.

      NOTE
      The uWatts display requires devices with Fabric OS 6.1.0 and later. Devices running Fabric OS 6.0.0 and earlier only display dBm.

    - **Transceiver Temp**—The temperature of the SFP transceiver.
    - **Vendor**—The vendor of the SFP.
    - **Vendor OUI**—The vendor's organizational unique identifier (OUI).
    - **FC Speed**—The FC port speed; for example, 400 Mbps.
    - **Distance**—The length of the fiber optic cable.
    - **Vendor PN**—The part number of the SFP.
    - **Vendor Rev**—The revision number of the SFP.
    - **Serial #**—The serial number of the SFP.
    - **Data Code**—The data code.
    - **Media Form Factor**—The type of media for the transceiver; for example, single mode.
    - **Connector**—The type of port connector.
    - **Wave Length**—The wave length.
    - **Encoding**—Displays how the fiber optic cable is encoded.
    - **Voltage (mVolts)**—The voltage across the port in mVolts.
3. Sort the results by clicking on the column header.
4. Rearrange the columns by dragging and dropping the column header.
5. Click **Cancel** to close the **Port Optics (SFP)** dialog box.

Refreshing port optics

To refresh port optics, click **Refresh**.

The Management application retrieves updated port optic information.

Port Auto Disable

The **Port Auto Disable** dialog box allows you to enable and disable the port auto disable flag on individual FC_ports or on all ports on a selected device, as well as unblock currently blocked ports.

NOTE
The device must be running Fabric OS 6.3 or later.

Viewing the port auto disable status

NOTE
The device must be running Fabric OS 6.3 or later.

1. Select **Configure > Port Auto Disable**.

   The **Port Auto Disable** dialog box displays.

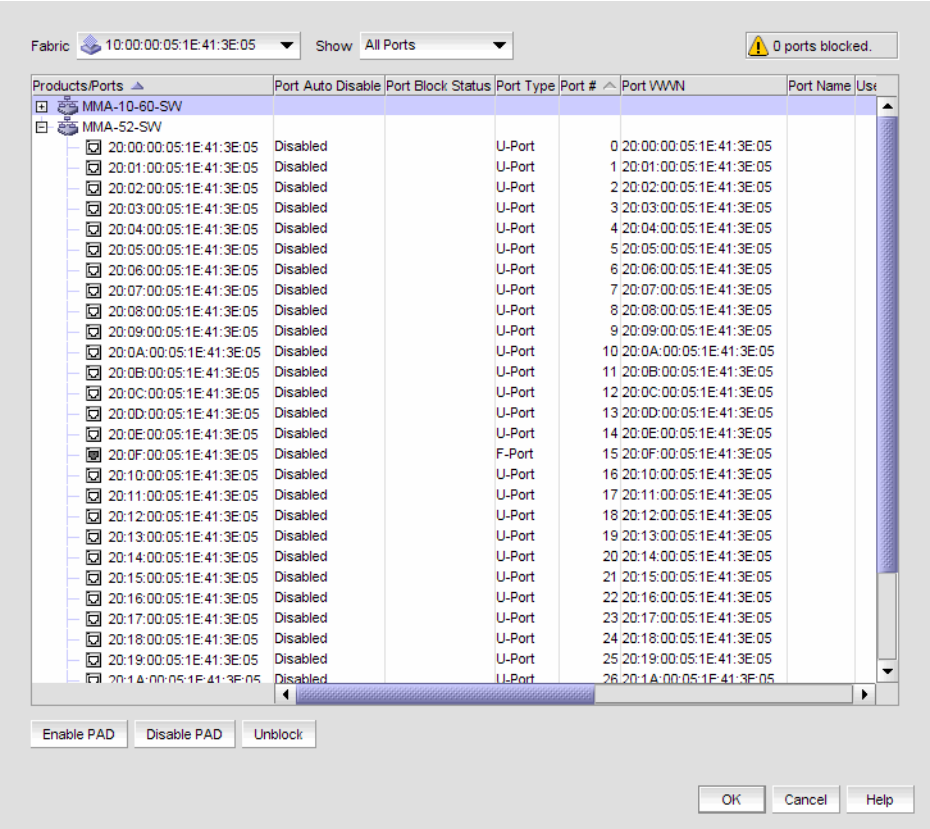


FIGURE 58 **Port Auto Disable dialog box**

2. Review the port status and other information:
   - **Products/Ports** tree—Displays devices and associated ports. Also, displays a Warning icon for blocked FC ports (displayed with the port icon).
   - **Port Auto Disable**—Displays whether Port Auto Disable is currently enabled or disabled.
   - **Port Block Status**—Displays whether the port is currently blocked.

- **Port Type**—Displays the port type.
- **Port Number**—Displays the port number.
- **Port WWN**—Displays the port world wide name.
- **Port Name**—Displays the port name.
- **User Port #**—Displays the user port number.
- **PID**—Displays the port identifier.
- **Connected Port #**—Displays the connected port number.
- **Connected Port WWN**—Displays the connected port world wide name.
- **Connected Port Name**—Displays the connected port name.

3. Click **OK** on the **Port Auto Disable** dialog box.

Enabling port auto disable on individual ports

NOTE
The device must be running Fabric OS 6.3 or later.

1. Select **Configure > Port Auto Disable**.

   The **Port Auto Disable** dialog box displays.

2. Select the fabric on which you want to enable port auto disable (PAD) from the **Fabric** list.
3. Choose one of the following options from the **Show** list to filter the port list:
   - **All Ports** (default)—Displays all ports in the fabric.
   - **Disabled PAD**—Displays only ports where PAD is enabled.
4. Select the ports on which you want to enable PAD.
5. Click **Enable PAD**.
6. Click **OK** on the **Port Auto Disable** dialog box.

Enabling port auto disable on all ports on a device

NOTE
The device must be running Fabric OS 6.3 or later.

1. Select **Configure > Port Auto Disable**.

   The **Port Auto Disable** dialog box displays.

2. Select the fabric on which you want to enable port auto disable (PAD) from the **Fabric** list.
3. Select **All Ports** from the **Show** list.
4. Select the device on which you want to enable PAD on all ports.
5. Click **Enable PAD**.
6. Click **OK** on the **Port Auto Disable** dialog box.

Disabling port auto disable on individual ports

NOTE
The device must be running Fabric OS 6.3 or later.

1. Select **Configure > Port Auto Disable**.

   The **Port Auto Disable** dialog box displays.
2. Select the fabric on which you want to disable port auto disable (PAD) from the **Fabric** list.
3. Choose one of the following options from the **Show** list to filter the port list:
   - **All Ports** (default)—Displays all ports in the fabric.
   - **Enabled PAD**—Displays only ports where PAD is enabled.
4. Select the ports on which you want to disable PAD.
5. Click **Disable PAD**.
6. Click **OK** on the **Port Auto Disable** dialog box.

Disabling port auto disable on all ports on a device

NOTE
The device must be running Fabric OS 6.3 or later.

1. Select **Configure > Port Auto Disable**.

   The **Port Auto Disable** dialog box displays.
2. Select the fabric on which you want to disable port auto disable (PAD) from the **Fabric** list.
3. Select **All Ports** from the **Show** list.
4. Select the device on which you want to disable PAD on all ports.
5. Click **Disable PAD**.
6. Click **OK** on the **Port Auto Disable** dialog box.

Unblocking ports

NOTE
The device must be running Fabric OS 6.3 or later.

1. Select **Configure > Port Auto Disable**.

   The **Port Auto Disable** dialog box displays.
2. Select the fabric on which you want to enable port auto disable (PAD) from the **Fabric** list.
3. Select **Blocked Ports** from the **Show** list.
4. Select the device on which you want to enable PAD on all ports.
5. Click **Enable PAD**.
6. Click **OK** on the **Port Auto Disable** dialog box.

Device Technical Support

You can use Technical Support to collect supportSave data (such as, RASLOG, TRACE and so on) and switch events from Fabric OS devices.

You can gather technical data for M-EOS devices using the device's Element Manager.

To gather technical support information for the Management application server, refer to "Capturing technical support information" on page 128.

Scheduling technical support information collection

NOTE
The switch must be running Fabric OS 5.2.X or later to collect technical support data.

NOTE
You must have the SupportSave privilege to perform this task.

To capture technical support and event information for specified devices, complete the following steps.

1. Select **Monitor > Technical Support > SupportSave**.

   The **Technical SupportSave** dialog box displays.

2. Click the **Schedule** tab.
3. Select the **Enable scheduled Technical Support Data** check box.
4. Select how often you want the scheduled collection to occur from the **Frequency** list.
5. Select the start date for the scheduled collection from the **Start Date** list.

   This list is only available when you select Weekly or Monthly from the **Frequency** list.

6. Select the time you want the scheduled collection to begin from the **Start Time Hour** and **Minute** lists.
7. Right-click in the **Available Switches** table and select **Expand All**.
8. Select the switches you want to collect data for in the **Available Switches** table and click the right arrow to move them to the **Selected Switches** table.
9. Select how often you want to purge the support data from the **Purge Support Data** list.
10. Click **OK** on the **Technical SupportSave** dialog box.
11. Click **OK** on the confirmation message.

    Data collection may take 20-30 minutes for each selected switch. This estimate my increase depending on the number of switches selected. Check the Master Log for status information.

Starting immediate technical support information collection

NOTE
The switch must be running Fabric OS 5.2.X or later to collect technical support data.

NOTE
The HBA must be a managed Brocade HBA.

NOTE
You must have the SupportSave privilege to perform this task.

To capture technical support and event information for specified devices, complete the following steps.

1. Select **Monitor > Technical Support > SupportSave**.

   The **Technical SupportSave** dialog box displays.

2. Click the **Generate Now** tab, if necessary.
3. Click the **Switches** tab, if necessary, and complete the following steps.
   a. Right-click in the **Available Switches** table and select **Expand All**.
   b. Select the switches you want to collect data for in the **Available Switches** table and click the right arrow to move them to the **Selected Switches and Hosts** table.
4. Click the **Hosts** tab, if necessary, and complete the following steps.
   a. Right-click in the **Available Hosts** table and select **Expand All**.
   b. Select the switches you want to collect data for in the **Available Switches** table and click the right arrow to move them to the **Selected Switches and Hosts** table.
5. Click **OK** on the **Technical SupportSave** dialog box.
6. Click **OK** on the confirmation message.

   Data collection may take 20-30 minutes for each selected switch. This estimate my increase depending on the number of switches selected. Check the Master Log for status information.

Viewing technical support information

To view technical support information, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

   The **Repository** dialog box displays.

2. Choose from one of the following options:
   - Select the **Switches** tab to view technical support information on switches.
   - Select the **Hosts** tab to view technical support information on hosts.
3. Click **View** to view the repository in an Internet browser window.

   The technical support information displays in an Internet browser window.

4. Click the appropriate link to view details.
5. Click **OK** on the **Repository** dialog box.

E-mailing technical support information

To e-mail technical support information, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

   The **Repository** dialog box displays.
2. Choose from one of the following options:
   - Select the **Switches** tab to e-mail technical support information on switches.
   - Select the **Hosts** tab to e-mail technical support information on hosts.
3. Select the file you want to e-mail in the table.
4. Click **E-mail** to e-mail the switch event and supportsave files (zip).

   You must configure the Management application e-mail server before you can define the e-mail action. For more information, refer to "Configuring e-mail notification" on page 196.

   The **E-mail** dialog box displays.
5. Enter the e-mail address of the person to receive the e-mail in the **To** field.
6. Enter your e-mail address in the **From** field.
7. Click **OK**.

   The e-mail is sent and the **Repository** dialog box closes automatically.

Deleting technical support files from the repository

To delete a technical support file from the repository, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

   The **Repository** dialog box displays.
2. Choose from one of the following options:
   - Select the **Switches** tab to delete technical support information on switches.
   - Select the **Hosts** tab to delete technical support information on hosts.
3. Select the file you want to delete in the table.
4. Click **Delete**.
5. Click **OK** on the **Technical SupportSave** dialog box.
6. Click **OK** on the confirmation message.

Failure data capture

You can use Upload Failure Data Capture to enable, disable, and purge failure data capture files as well as configure the FTP Host for the switch.

NOTE
Upload Failure Data Capture is only supported on Fabric OS devices.

Enabling failure data capture

1. Select **Monitor > Technical Support > Upload Failure Data Capture**.

   The **Upload Failure Data Capture** dialog box displays.

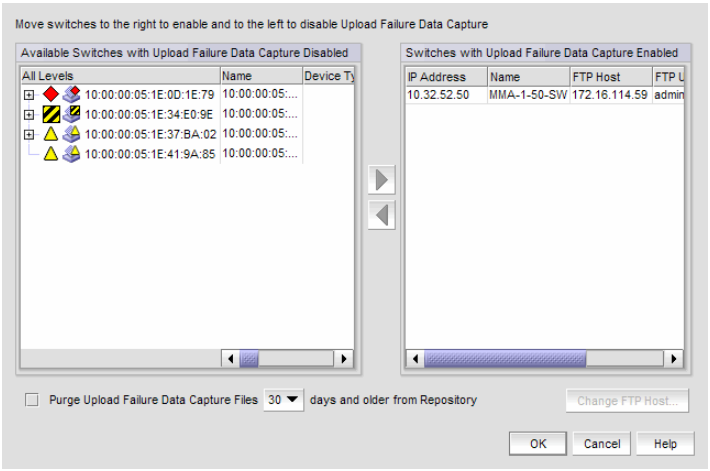


FIGURE 59 **Upload Failure Data Capture dialog box**

2. Select a one or more devices on which you want to enable automatic trace dump from the **Available Switches with Upload Failure Data Capture Disabled** table.
3. Click the right arrow button.

   The selected devices move from the **Available Switches with Upload Failure Data Capture Disabled** table to the **Switches with Upload Failure Data Capture Enabled** table.
4. Click **OK** on the **Upload Failure Data Capture** dialog box.
5. Click **OK** on the confirmation message, if necessary.

Disabling failure data capture

NOTE
Upload Failure Data Capture is only supported on Fabric OS devices.

1. Select **Monitor > Technical Support > Upload Failure Data Capture**.

   The **Upload Failure Data Capture** dialog box displays.

2. Select one or more devices on which you want to disable automatic trace dump from the **Available Switches with Upload Failure Data Capture Enabled** table.
3. Click the left arrow button.

   The selected devices move from the **Switches with Upload Failure Data Capture Enabled** table to the **Available Switches with Upload Failure Data Capture Disabled** table.

4. Click **OK** on the **Upload Failure Data Capture** dialog box.
5. Click **OK** on the confirmation message, if necessary.

Purging failure data capture files

NOTE
Upload Failure Data Capture is only supported on Fabric OS devices.

1. Select **Monitor > Technical Support > Upload Failure Data Capture**.

   The **Upload Failure Data Capture** dialog box displays.

2. Select the **Purge Upload Failure Data Capture Files** check box to enable purging the trace dump files.
3. Select how often (days) you want to purge the trace dump data from the **Purge Upload Failure Data Capture Files** list.
4. Click **OK** on the **Upload Failure Data Capture** dialog box.

Configuring the failure data capture FTP server

NOTE
Upload Failure Data Capture is only supported on Fabric OS devices.

1. Select **Monitor > Technical Support > Upload Failure Data Capture**.

   The **Upload Failure Data Capture** dialog box displays.

2. Select a device from the **Available Switches with Upload Failure Data Capture Enabled** table.

3. Click **Change FTP Host.**

   The **Change FTP Server** dialog box displays.

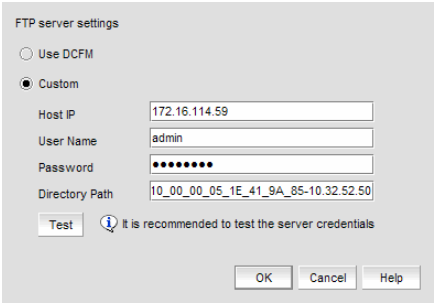


FIGURE 60 Change FTP Server dialog box

4. Choose one of the following options:
   - Select the **Use** <*Management_Application*> option to use the Management application FTP server.
   - Select the **Custom** option and complete the following steps to configure a FTP server for the selected device.
     a. Enter the server's IP address in the **Host IP** field.
     c. Enter a user name for the server in the **User Name** field.
     d. Enter a password for the server in the **Password** field.
     e. Enter the path to where the trace dump data is saved in the **Directory Path** field.
5. Click **Test** to test the server credentials.
6. Click **OK** on the **Change FTP Host** dialog box.
7. Click **OK** on the **Upload Failure Data Capture** dialog box.
8. Click **OK** on the confirmation message, if necessary.

Viewing the upload failure data capture repository

NOTE
Upload Failure Data Capture is only supported on Fabric OS devices.

1. Select **Monitor > Technical Support > View Repository**.

   The **Repository** dialog box displays.

2. Select the trace dump file you want to view from the **Available Support and Upload Failure Data Capture Files** table.
3. Click **View**.

   The Upload Failure Data Capture repository displays.

Chapter

6

Fault Management

In this chapter

- Fault management overview. 171
- Event logs. 172
- Event policies. 179
- Event notification. 196
- SNMP trap and informs registration and forwarding 199
- Syslog forwarding. 204

Fault management overview

Fault management enables you to monitor your SAN using the following methods:

- Monitor logs for specified conditions and notify you or run a script when the specified condition is met.
- Create event-based policies, which contain an event trigger and action.
- Configure E-mail event notification.
- Listen, forward, and process SNMP traps from Fabric OS switches, which eliminates the need to poll switches for events.
- Receive and forward Syslog messages from Fabric OS switches and Brocade HBAs (managed using HCM Agent).

Fault management also supports application events.

Event logs

The Management application provides a variety of logs through which you can monitor the SAN.

You can view all events that take place in the SAN through the Master Log at the bottom of the main window. You can also view a specific log by selecting an option from the **Monitor** menu's **Logs** submenu. The logs are described in the following list:

- **Audit Log.** Displays all 'Application Events' raised by the application modules and all Audit Syslog messages from the switches and Brocade HBAs.
- **Event Log.** Displays all 'Product Event' type events from all discovered switches and Brocade HBAs.
- **Fabric Log.** Displays 'Product Events', 'Device Status', and 'Product Audit' type events for all discovered fabrics.
- **FICON Log.** Displays all the 'RLIR' and 'LRIR' type events, for example, 'link incident' type events.
- **Product Status Log.** Displays events which indicate a change in Switch Status for all discovered switches and Brocade HBAs.
- **Security Log.** Displays all security events for the discovered switches.
- **Syslog Log.** Displays syslog messages from switches and HBAs.

The Management application also has an event notification feature. By configuring event notification, you can specify when the application should alert you of an event. For details, refer to "Configuring e-mail notification" on page 196.

For information about the Master Log interface, fields, and icons, refer to "Master Log" on page 13.

Viewing event logs

You can view log data through the Master Log on the main window. However, if you want to see only certain types of events, for example only security events, open a specific log through the **Logs** dialog box.

NOTE
You can also launch the Fabric logs and the Product Status logs from the Status bar.

To view a log, complete the following steps.

1. Select **Monitor > Logs >** <*Log_Type*>.

   The <*Log_Type*> **Logs** dialog box displays the kind of log you selected.

2. Review the information in the log.
3. Click **Close**.

Copying part of a log entry

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy part of a log, complete the following steps.

1. Select **Monitor > Logs >** <*Log_Type*>.

   The <*Log_Type*> **Logs** dialog box displays the kind of log you selected.

2. Select the rows you want to copy.
   - To select contiguous rows, select the first row you want to copy, press Shift, and click the contiguous row or rows you want to copy.
   - To select non-contiguous rows, select the first row you want to copy, press CTRL, and click the additional row or rows you want to copy.
3. Right-click one of the selected rows and select **Copy Rows**.
4. Open the application to which you want to paste the data.
5. Click where you want to paste the data.
6. Press CTRL+V (or select **Edit > Paste** from the other application).

   All data and column headings are pasted.

7. Click **Close** to close the dialog box.

Copying an entire log entry

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy a log, complete the following steps.

1. Select **Monitor > Logs >** <*Log_Type*>.

   The <*Log_Type*> **Logs** dialog box displays the kind of log you selected.

2. Right-click a row and select **Copy Table**.
3. Open the application to which you want to paste the data.
4. Click where you want to paste the data.
5. Press CTRL+V (or select **Edit > Paste** from the other application).

   All data and column headings are pasted.

6. Click **Close** to close the dialog box.

Exporting the entire log

You can export the log data to a tab delimited text file.

To export a log, complete the following steps.

1. Select **Monitor > Logs >** <*Log_Type*>.

   The <*Log_Type*> **Log** dialog box displays the kind of log you selected.

2. Right-click a row and select **Export Table**.

   The **Save table to a tab delimited file** dialog box displays.

3. Browse to the location where you want to export the data.
4. Enter a name for the file in the **File Name** field.
5. Click **Save**.

   All data and column headings are exported to the text file.

6. Click **Close** to close the dialog box.

E-mailing all event details from the Master Log

NOTE
You must configure e-mail notification before you can e-mail event details from the Master Log. To configure e-mail notification, refer to "Configuring e-mail notification" on page 196.

To e-mail event details from the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **E-mail > All.**

   The **E-mail** dialog box displays.

3. Enter the e-mail address of the person to receive the e-mail in the **To** field.
4. Enter your e-mail address in the **From** field.
5. Click **OK**.

E-mailing selected event details from the Master Log

NOTE
You must configure e-mail notification before you can e-mail event details from the Master Log. To configure e-mail notification, refer to "Configuring e-mail notification" on page 196.

To e-mail event details from the Master Log, complete the following steps.

1. Select the events that you want to e-mail.
2. Right-click the selected events in the Master Log.
3. Select **E-mail > Selection.**

   The **E-mail** dialog box displays.

4. Enter the e-mail address of the person to receive the e-mail in the **To** field.

5. Enter your e-mail address in the **From** field.
6. Click **OK**.

E-mailing a range of event details from the Master Log

NOTE
You must configure e-mail notification before you can e-mail event details from the Master Log. To configure e-mail notification, refer to "Configuring e-mail notification" on page 196.

To e-mail event details from the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **E-mail > Date.**

   The **E-mail** dialog box displays.
3. Select the date range for the event details you want to e-mail in the **Range** from and to fields.
4. Enter the e-mail address of the person to receive the e-mail in the **To** field.
5. Enter your e-mail address in the **From** field.
6. Click **OK**.

Displaying event details from the Master Log

You can view detailed information for an event.

To display event details from the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **Display Details**.

   The **Event Details** dialog box displays.
3. Review the information.

TABLE 25 Event Details

Event Field	Description
Count	Number of times this event occurred on the host.
Resolved	Whether or not the event has been resolved.
Message	The message associated with the event.
Time (Switch)	The time the event occurred and the switch on which it occurred.
Probable Cause	The probable cause of the event.
Module Name	The module name.
Event Source	The event source.
Audit	The audit.
Status	The switch operational status.
Severity	The event severity.
Source Name	The source of the event.

TABLE 25 Event Details

Event Field	Description
Virtual Fabric ID	The virtual fabric identifier.
Message ID	The message text.
Recommended Action	The recommended action.
Contributors	The contributor to this event.
Time (Host)	The time this event occurred and the host on which it occurred.

4. Click **Close** to close the **Event Details** dialog box.

Copying part of the Master Log

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy part of the Master Log, complete the following steps.

1. Select the rows you want to copy in the Master Log.
   - To select contiguous rows, select the first row you want to copy, press Shift, and click the contiguous row or rows you want to copy.
   - To select non-contiguous rows, select the first row you want to copy, press CTRL, and click the additional row or rows you want to copy.
2. Right-click one of the selected rows and select **Table > Copy Rows**.
3. Open the application to which you want to paste the data.
4. Click where you want to paste the data.
5. Press CTRL+V (or select **Edit > Paste** from the other application).

   All data and column headings are pasted.

Copying the entire Master Log

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **Table > Copy Table**.
3. Open the application to which you want to paste the data.
4. Click where you want to paste the data.
5. Press CTRL+V (or select **Edit > Paste** from the other application).

   All data and column headings are pasted.

Exporting the Master Log

You can export the Master Log to a tab delimited text file. Use this to analyze or store the data using another tool.

To export the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **Table > Export Table**.

   The **Save table to a tab delimited file** dialog box displays.
3. Browse to the location where you want to export the data.
4. Enter a name for the file in the **File Name** field.
5. Click **Save**.

   All data and column headings are exported to the text file.
6. Click **Close** to close the dialog box.

Filtering events in the Master Log

You can filter the events that display in the Master Log on the main window. By default, all event types display in the **Selected Events** table.

For more information about the Master Log, refer to "Master Log" on page 13.

NOTE
The e-mail filter in the Management application is overridden by the firmware e-mail filter. When the firmware determines that certain events do not receive e-mail notification, an e-mail is not sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box.

To filter events, complete the following steps.

1. Click the **Filter** hyper link in the Master Log.

   The **Define Filter** dialog box displays (Figure 68).

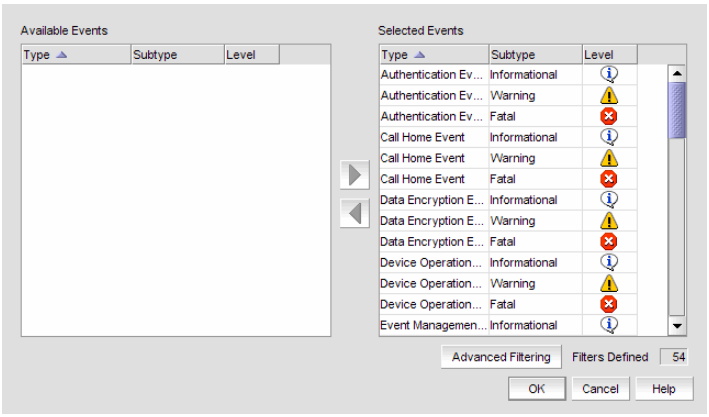


FIGURE 61 Define Filter Dialog Box

2. Select from the following to include or exclude event types.
   - To include an event type in the filter, select the event from the **Available Events** table and click the right arrow.
   - To exclude an event type from the filter, select the event from the **Selected Events** table and click the left arrow.
3. Click **OK**.
4. Select one of the following to determine what view to filter events.
   - Select the **Filter** check box to view only the events specified in the **Define Filter** dialog box, regardless of the current view.
   - Select the **Only events for current view** check box to view only the events specified in the **Define Filter** dialog box for products in the current view.

NOTE
Selecting these options only filters product-specific events.

Clear both the **Filter** and **Only events in current view** check boxes to turn off the filter and view all events.

Event policies

You can create policies for events you want to monitor. A policy is the mechanism defined by you that identifies the response to specific event types. You can customize the event management policy using triggers and actions, which are explained in this section. You can create a maximum of 10 policies at a time.

Policy types

You can configure event policies for the following policy types:

- Event — use to configure triggers and actions for the following Event types.
- ISL Offline — use to configure triggers and actions for ISL.
- PM Threshold Crossed — use to configure triggers and actions for performance thresholds.
- Security Violation — use to configure triggers and actions for security violations.

Event types

You can configure triggers and actions for the following event types:

- Authentication Event — occurs when an authentication event has been triggered.
- Call Home Event — occurs when a call home event has been triggered.
- Data Encryption Event — occurs when a data encryption event has been triggered.
- Device Status Event — notifies you of the operational status of SAN products.
- Fabric Event — notifies you of fabric changes.
- Fault Management Event — occurs when an event policy has been triggered.
- Link Incident Event — notifies you of changes to the link status.
- Performance Event — occurs when the performance at a switch port crosses a defined threshold.
- Product Audit Event — occurs when a target product is audited.
- Product Event — notifies you when the product status changes.
- Product Open Trunking Event — occurs when a device open trunking event has been triggered.
- Product State Event — occurs when a device or connection changes to Up or Down.
- Product Threshold Alert Event — notifies you when a threshold alert has been reached.
- Security Event — notifies you when a product's security level changes.
- Software Exception Event — occurs when a software exception event has been triggered.
- Tech Support Event — occurs when a technical support event is triggered.
- User Action Event — occurs when you change a setting in the Server.
- Zoning Event — occurs when a zoning event has been triggered.

Policy triggers

A trigger is a logical filter that determines which conditions will initiate a set of predefined actions. You can set multiple triggers. The Management application enables you to set the following triggers:

- **IP Address** — Initiates the defined action when the IP address of a device is encountered.
- **Node WWN** — Initiates the defined action when the Node WWN of a device is encountered.
- **Name** — Initiates the defined action when the Name (user-defined) of a device is encountered.

Policy actions

You can automate tasks that you perform on the SAN by configuring multiple actions to be performed when an associated trigger is fired. The following actions are available:

- **Broadcast Message** — Displays a message to all open Clients.
- **Launch Script** — Launches the specified application using a script.

  NOTE
  Launch scripts with a user interface are not supported.

- **Send E-mail** — Sends an e-mail message to specified recipients.
- **Capture Support Data (FOS)** — Triggers supportSave capture.

Adding an event policy

To add an event policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Click **Add**.

   The **Add Event Policy** dialog box displays.

3. Enter a name (255 characters maximum) for the policy in the **Name** field.

   Policy names must be unique; however, they are case insensitive.

4. Enter a description (255 characters maximum) for the policy in the **Description** field.

5. Select **Event** from the **Policy Type** list.

6. Select an event type from the **Event Type** list.

   For a list of event types, refer to "Event types" on page 179.

7. Select an event level (ERROR, WARNING, or INFO) from the **Event Level** list.

8. Enter all or part of the event description text (255 characters maximum) in the **Description Contains** field.

   This entry can be from the start, middle, or end of the event description. If the entry matches or is part of the event description, the policy is triggered.

9. Enter all or part of the message ID associated with SNMP traps and Syslog messages in the **Message ID** field.

   If the entry matches or is part of the message ID, the policy is triggered.

10. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.

    The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches in the event and all other conditions are met, an action is triggered.

    IP addresses can either be in IPv4 or IPv6 format and must be complete.

    A Node WWN is accepted with or without the colon.

11. Enter a value (between 2 and 999) in the **Count** field.
12. Enter a value (between 1 and 999) in the **Duration** field.
13. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

    The maximum duration is 30 minutes.

14. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

    For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

15. Click **OK** on the **Add Event Policy** dialog box.
16. Select the **Active** check box for the policy you want to activate.
17. Click **OK** on the **Event Policies** dialog box.

Adding an ISL offline policy

To add an ISL offline policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Click **Add**.

   The **Add Event Policy** dialog box displays.

3. Enter a name (255 characters maximum) for the policy in the **Name** field.

   Policy names must be unique; however, they are case insensitive.

4. Enter a description (255 characters maximum) for the policy in the **Description** field.
5. Select **ISL Offline** from the **Policy Type** list.

6. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.

   The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

   IP addresses can either be in IPv4 or IPv6 format and must be complete.

   A Node WWN is accepted with or without the colon.

7. Enter a value (between 2 and 999) in the **Count** field.
8. Enter a value (between 1 and 999) in the **Duration** field.
9. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

   The maximum duration is 30 minutes.

10. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

    For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

11. Click **OK** on the **Add Event Policy** dialog box.
12. Select the **Active** check box for the policy you want to activate.
13. Click **OK** on the **Event Policies** dialog box.

Adding a PM threshold crossed policy

To add a PM threshold crossed policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Click **Add**.

   The **Add Event Policy** dialog box displays.

3. Enter a name (255 characters maximum) for the policy in the **Name** field.

   Policy names must be unique; however, they are case insensitive.

4. Enter a description (255 characters maximum) for the policy in the **Description** field.
5. Select **PM Threshold Crossed** from the **Policy Type** list.
6. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.

   The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

   IP addresses can either be in IPv4 or IPv6 format and must be complete.

   A Node WWN is accepted with or without the colon.

7. Enter a value (between 2 and 999) in the **Count** field.
8. Enter a value (between 1 and 999) in the **Duration** field.

9. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

   The maximum duration is 30 minutes.

10. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

    For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

11. Click **OK** on the **Add Event Policy** dialog box.
12. Select the **Active** check box for the policy you want to activate.
13. Click **OK** on the **Event Policies** dialog box.

Adding a security violation policy

To add a security violation policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Click **Add**.

   The **Add Event Policy** dialog box displays.

3. Enter a name (255 characters maximum) for the policy in the **Name** field.

   Policy names must be unique; however, they are case insensitive.

4. Enter a description (255 characters maximum) for the policy in the **Description** field.
5. Select **Security Violation** from the **Policy Type** list.
6. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.

   The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

   IP addresses can either be in IPv4 or IPv6 format and must be complete.

   A Node WWN is accepted with or without the colon.

7. Enter a value (between 2 and 999) in the **Count** field.
8. Enter a value (between 1 and 999) in the **Duration** field.
9. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

   The maximum duration is 30 minutes.

10. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

    For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

11. Click **OK** on the **Add Event Policy** dialog box.
12. Select the **Active** check box for the policy you want to activate.
13. Click **OK** on the **Event Policies** dialog box.

Defining the broadcast message action

You can define the content of the broadcast message that occurs when a policy is triggered. You can only edit actions from the **Add Event Policy**, **Duplicate Event Policy**, or **Edit Event Policy** dialog boxes.

For step-by-step instructions on adding or editing an event policy, refer to "Adding an event policy" on page 180, "Adding an ISL offline policy" on page 181, "Adding a PM threshold crossed policy" on page 182, or "Adding a security violation policy" on page 183.

For step-by-step instructions on duplicating an event policy, refer to "Duplicating an event policy" on page 188, "Duplicating an ISL offline policy" on page 189, "Duplicating a PM threshold crossed policy" on page 190, or "Duplicating a security violation policy" on page 191.

For step-by-step instructions on editing an event policy, refer to "Editing an event policy" on page 192, "Editing an ISL offline policy" on page 193, "Editing a PM threshold crossed policy" on page 194, or "Editing a security violation policy" on page 195.

To define the broadcast message, complete the following steps.

1. Select **Broadcast Message** from the **Actions** list.
2. Click **Change**.

   The **Broadcast Message** dialog box displays.
3. Select a severity (error, warning, or informational) for the message from the **Severity** list.
4. Enter a message to be displayed when the policy is triggered in the **Message Content** field.

   You can enter 256 characters for the broadcast message. The following special characters are not allowed: ~ ‘ ! @ $ ^ & + = { } [ ] | \ ‘ < > / “
5. Click **OK** on the **Broadcast Message** dialog box.
6. Click **OK** on the **Add**, **Duplicate**, or **Edit Event Policy** dialog box.

Defining the launch script action

NOTE
Launch scripts with a user interface are not supported.

You can define the path to the script that is launched when a policy is triggered. When the script launches, the Management application does not verify the existence of the script.

The script must have the following characteristics:

- It must reside on the Management application server.
- It must be capable of being executed by the OS where the Management application server is installed and it must be a valid binary for that OS (Windows, Solaris, or Linux).
- It must be able to receive a command-line argument from the Management application. The argument is the name of the XML file that generates when an event occurs.

You can only edit actions from the **Add Event Policy**, **Duplicate Event Policy**, or **Edit Event Policy** dialog boxes.

For step-by-step instructions on adding or editing an event policy, refer to "Adding an event policy" on page 180, "Adding an ISL offline policy" on page 181, "Adding a PM threshold crossed policy" on page 182, or "Adding a security violation policy" on page 183.

For step-by-step instructions on duplicating an event policy, refer to "Duplicating an event policy" on page 188, "Duplicating an ISL offline policy" on page 189, "Duplicating a PM threshold crossed policy" on page 190, or "Duplicating a security violation policy" on page 191.

For step-by-step instructions on editing an event policy, refer to "Editing an event policy" on page 192, "Editing an ISL offline policy" on page 193, "Editing a PM threshold crossed policy" on page 194, or "Editing a security violation policy" on page 195.

To define the launch script path, complete the following steps.

1. Select **Launch Script** from the **Actions** list.
2. Click **Change**.

   The **Launch Script** dialog box displays.
3. Enter the full path (including executable) of the launch script in the **File Name** field.

   NOTE
   Launch scripts with a user interface are not supported.

   You must enter a fully qualified path on the Management application Server for Windows (for example, C:\Program Files\<*Management_Application_Name*> 10.X.X\bin\xyz.bat) as well as Linux and Solaris (for example, /etc/proc/sbin/script.sh).
4. Click **OK** on the **Launch Script** dialog box.

   NOTE
   The Management application does not verify that the file name exists in the specified folder.
5. Click **OK** on the **Add**, **Duplicate**, or **Edit Event Policy** dialog box.

Defining the send e-mail action

You can define the content of the e-mail message that occurs when a policy is triggered. You can only edit actions from the **Add Event Policy**, **Duplicate Event Policy**, or **Edit Event Policy** dialog boxes.

For step-by-step instructions on adding or editing an event policy, refer to "Adding an event policy" on page 180, "Adding an ISL offline policy" on page 181, "Adding a PM threshold crossed policy" on page 182, or "Adding a security violation policy" on page 183.

For step-by-step instructions on duplicating an event policy, refer to "Duplicating an event policy" on page 188, "Duplicating an ISL offline policy" on page 189, "Duplicating a PM threshold crossed policy" on page 190, or "Duplicating a security violation policy" on page 191.

For step-by-step instructions on editing an event policy, refer to "Editing an event policy" on page 192, "Editing an ISL offline policy" on page 193, "Editing a PM threshold crossed policy" on page 194, or "Editing a security violation policy" on page 195.

You must configure the Management application e-mail server before you can define the e-mail action. For more information, refer to "Configuring e-mail notification" on page 196.

To define the e-mail message, complete the following steps.

1. Select **Send E-mail** from the **Actions** list.
2. Click **Change**.

   The **Send E-Mail** dialog box displays.
3. Enter the e-mail address of the person you want to receive this message when the trigger occurs in the **To** field.
4. Enter your e-mail address in the **From** field.
5. Enter a subject for the e-mail message in the **Subject** field.
6. Enter a message to be displayed when the policy is triggered in the **Message** field.

   You can enter 256 characters for the e-mail message. The following special characters are not allowed: ~ ‘ ! @ $ ^ & + = { } [ ] | \ ‘ < > / : “
7. Click **OK** on the **Send E-Mail** dialog box.
8. Click **OK** on the **Add**, **Duplicate**, or **Edit Event Policy** dialog box.

Configuring support data capture action

You can configure the Management application to start supportSave capture on Fabric OS devices when a policy is triggered. You can only edit actions from the **Add Event Policy**, **Duplicate Event Policy**, or **Edit Event Policy** dialog boxes.

For step-by-step instructions on adding or editing an event policy, refer to "Adding an event policy" on page 180, "Adding an ISL offline policy" on page 181, "Adding a PM threshold crossed policy" on page 182, or "Adding a security violation policy" on page 183.

For step-by-step instructions on duplicating an event policy, refer to "Duplicating an event policy" on page 188, "Duplicating an ISL offline policy" on page 189, "Duplicating a PM threshold crossed policy" on page 190, or "Duplicating a security violation policy" on page 191.

For step-by-step instructions on editing an event policy, refer to "Editing an event policy" on page 192, "Editing an ISL offline policy" on page 193, "Editing a PM threshold crossed policy" on page 194, or "Editing a security violation policy" on page 195.

To configure the Management application to start supportSave on Fabric OS devices, complete the following steps.

NOTE
If you select **User Action Event** or **Tech Support Event** from the **Event Type** list, **Capture Support Data (FOS)** cannot be configured to start supportSave capture.

1. Select **Capture Support Data (FOS)** from the **Actions** list.
2. Click **OK** on the message.

   Note that capture support data is only triggered for Fabric OS switch events.
3. Click **OK** on the **Add**, **Duplicate**, or **Edit Event Policy** dialog box.

Activating a policy

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.
2. Select the **Active** check box for each policy you want to activate.

   If the policy actions have not been selected an error message displays. For step-by-step instructions, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, or "Defining the send e-mail action" on page 186.
3. Click **OK** on the **Event Policies** dialog box.

Deactivating a policy

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.
2. Clear the **Active** check box for each policy you want to deactivate.
3. Click **OK** on the **Event Policies** dialog box.

Deleting a policy

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Select the policy you want to delete.

   Press Ctrl and then click to select more than one policy.

3. Click **Delete**.

4. Click **OK** on the **Event Policies** dialog box.

Duplicating an event policy

To duplicate an event policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Select the policy you want to duplicate in the **Policies** table.

3. Click **Duplicate**.

   The **Duplicate Event Policy** dialog box displays.

4. Enter a name (255 characters maximum) for the policy in the **Name** field.

   Policy names must be unique; however, they are case insensitive.

5. Edit the description (255 characters maximum) for the policy in the **Description** field.

6. Change the event type by selecting an event type from the **Event Type** list.

   For a list of event types, refer to "Event types" on page 179.

7. Change the event level by selecting an event level from the **Event Level** list.

8. Edit the event description text (255 characters maximum) in the **Description Contains** field.

   This entry can be from the start, middle, or end of the event description. If the entry matches or is part of the event description, the policy is triggered.

9. Edit the message ID associated with SNMP traps and Syslog messages in the **Message ID** field.

   If the entry matches or is part of the message ID, the policy is triggered.

10. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

    The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

    IP addresses can either be in IPv4 or IPv6 format and must be complete.

    A Node WWN is accepted with or without the colon.

11. Change the count value (between 2 and 999) in the **Count** field.
12. Change the duration value (between 1 and 999) in the **Duration** field.
13. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

    The maximum duration is 30 minutes.

14. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

    For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

15. Click **OK** on the **Edit Event Policy** dialog box.
16. Select the **Active** check box to activate the duplicated policy.
17. Click **OK** on the **Event Policies** dialog box.

Duplicating an ISL offline policy

To duplicate an ISL offline policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Select the policy you want to duplicate in the **Policies** table.
3. Click **Duplicate**.

   The **Duplicate Event Policy** dialog box displays.

4. Enter a name (255 characters maximum) for the policy in the **Name** field.

   Policy names must be unique; however, they are case insensitive.

5. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

   The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

   IP addresses can either be in IPv4 or IPv6 format and must be complete.

   A Node WWN is accepted with or without the colon.

6. Change the count value (between 2 and 999) in the **Count** field.
7. Change the duration value (between 1 and 999) in the **Duration** field.

8. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

   The maximum duration is 30 minutes.

9. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

   For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

10. Click **OK** on the **Edit Event Policy** dialog box.
11. Select the **Active** check box to activate the duplicated policy.
12. Click **OK** on the **Event Policies** dialog box.

Duplicating a PM threshold crossed policy

To duplicate a PM threshold crossed policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Select the policy you want to duplicate in the **Policies** table.
3. Click **Duplicate**.

   The **Duplicate Event Policy** dialog box displays.

4. Enter a name (255 characters maximum) for the policy in the **Name** field.

   Policy names must be unique; however, they are case insensitive.

5. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

   The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

   IP addresses can either be in IPv4 or IPv6 format and must be complete.

   A Node WWN is accepted with or without the colon.

6. Change the count value (between 2 and 999) in the **Count** field.
7. Change the duration value (between 1 and 999) in the **Duration** field.
8. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

   The maximum duration is 30 minutes.

9. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

   For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

10. Click **OK** on the **Add Event Policy** dialog box.

11. Select the **Active** check box to activate the duplicated policy.
12. Click **OK** on the **Event Policies** dialog box.

Duplicating a security violation policy

To duplicate a security violation policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.
2. Select the policy you want to duplicate in the **Policies** table.
3. Click **Duplicate**.

   The **Duplicate Event Policy** dialog box displays.
4. Enter a name (255 characters maximum) for the policy in the **Name** field.

   Policy names must be unique; however, they are case insensitive.
5. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.

   The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

   IP addresses can either be in IPv4 or IPv6 format and must be complete.

   A Node WWN is accepted with or without the colon.
6. Enter a value (between 2 and 999) in the **Count** field.
7. Enter a value (between 1 and 999) in the **Duration** field.
8. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

   The maximum duration is 30 minutes.
9. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

   For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.
10. Click **OK** on the **Add Event Policy** dialog box.
11. Select the **Active** check box to activate the duplicated policy.
12. Click **OK** on the **Event Policies** dialog box.

Editing an event policy

To edit an event policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Select the policy you want to edit in the **Policies** table.
3. Click **Edit**.

   The **Edit Event Policy** dialog box displays.

   NOTE
   You cannot edit the event policy name.

4. Edit the description (255 characters maximum) for the policy in the **Description** field.
5. Change the event type by selecting an event type from the **Event Type** list.

   For a list of event types, refer to "Event types" on page 179.

6. Change the event level by selecting an event level from the **Event Level** list.
7. Edit the event description text (255 characters maximum) in the **Description Contains** field.

   This entry can be from the start, middle, or end of the event description. If the entry matches or is part of the event description, the policy is triggered.

8. Edit the message ID associated with SNMP traps and Syslog messages in the **Message ID** field.

   If the entry matches or is part of the message ID, the policy is triggered.

9. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

   The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

   IP addresses can either be in IPv4 or IPv6 format and must be complete.

   A Node WWN is accepted with or without the colon.

10. Change the count value (between 2 and 999) in the **Count** field.
11. Change the duration value (between 1 and 999) in the **Duration** field.
12. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

    The maximum duration is 30 minutes.

13. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

    For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

14. Click **OK** on the **Edit Event Policy** dialog box.
15. Select the **Active** check box to activate the modified policy.
16. Click **OK** on the **Event Policies** dialog box.

Editing an ISL offline policy

To edit an ISL offline policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Select the policy you want to edit in the **Policies** table.

3. Click **Edit**.

   The **Edit Event Policy** dialog box displays.

4. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

   The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

   IP addresses can either be in IPv4 or IPv6 format and must be complete.

   A Node WWN is accepted with or without the colon.

5. Change the count value (between 2 and 999) in the **Count** field.

6. Change the duration value (between 1 and 999) in the **Duration** field.

7. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

   The maximum duration is 30 minutes.

8. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

   For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

9. Click **OK** on the **Edit Event Policy** dialog box.

10. Select the **Active** check box to activate the policy.

11. Click **OK** on the **Event Policies** dialog box.

Editing a PM threshold crossed policy

To edit a PM threshold crossed policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Select the policy you want to edit in the **Policies** table.

3. Click **Edit**.

   The **Edit Event Policy** dialog box displays.

4. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

   The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

   IP addresses can either be in IPv4 or IPv6 format and must be complete.

   A Node WWN is accepted with or without the colon.

5. Change the count value (between 2 and 999) in the **Count** field.

6. Change the duration value (between 1 and 999) in the **Duration** field.

7. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

   The maximum duration is 30 minutes.

8. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

   For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

9. Click **OK** on the **Add Event Policy** dialog box.

10. Select the **Active** check box to activate the policy.

11. Click **OK** on the **Event Policies** dialog box.

Editing a security violation policy

To edit a security violation policy, complete the following steps.

1. Select **Monitor > Event Policies**.

   The **Event Policies** dialog box displays.

2. Select the policy you want to edit in the **Policies** table.
3. Click **Edit**.

   The **Edit Event Policy** dialog box displays.

4. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.

   The trigger is limited to 255 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

   IP addresses can either be in IPv4 or IPv6 format and must be complete.

   A Node WWN is accepted with or without the colons.

5. Enter a value (between 2 and 999) in the **Count** field.
6. Enter a value (between 1 and 999) in the **Duration** field.
7. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

   The maximum duration is 30 minutes.

8. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

   For a list of the available actions, refer to "Policy actions" on page 180. To define an action, refer to "Defining the broadcast message action" on page 184, "Defining the launch script action" on page 185, "Defining the send e-mail action" on page 186, or "Configuring support data capture action" on page 187.

9. Click **OK** on the **Add Event Policy** dialog box.
10. Select the **Active** check box to activate the policy.
11. Click **OK** on the **Event Policies** dialog box.

Viewing events

The **All Events** dialog box enables you to view all events that have occurred on the selected switch, even events that were filtered using advanced filtering criteria.

To view events for a selected device, complete the following steps.

1. Right-click a switch from the device tree or connectivity map.
2. Select **Events** from the list.

   The **All Events** dialog box displays.

Event notification

The Management application records the SAN events in the Master Log. You can configure the application to send event notifications to e-mail addresses at certain time intervals. This is a convenient way to keep track of events that occur on the SAN.

Configuring e-mail notification

To send notification of events to users, complete the following steps.

1. Select **Monitor > Event Notification > E-mail**.

   The **E-mail Event Notification Setup** dialog box displays (Figure 62).

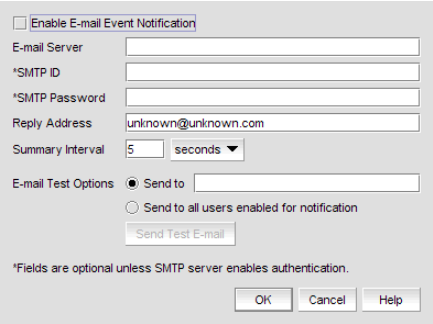


FIGURE 62 **E-mail Notification Setup Dialog Box**

2. Select the **Enable E-mail Event Notification** check box.
3. Enter the IP address or the name of the SMTP mail server that the Server can use to send the e-mail in the **E-mail Server** field.
4. Enter the authentication ID of the SMTP mail server in the **SMTP ID** field.

   NOTE
   This field is optional unless the SMTP server enables authentication.

5. Enter the authentication password of the SMTP mail server in the **SMTP Password** field.

   NOTE
   This field is optional unless the SMTP server enables authentication.

6. Enter the recipient's e-mail address in the **Reply Address** field.
7. Enter the length of time the application should wait between notifications in the **Summary Interval** field and list.

   Notifications are combined into a single e-mail and sent at each interval setting. An interval setting of zero causes notifications to be sent immediately.

   ATTENTION
   Setting too short an interval can cause the recipient's e-mail inbox to fill *very* quickly.

8. Select one of the following options:
   - Select **Send to** and enter an e-mail address for a user to send a test e-mail to a specific user.
   - Select **Send to all users enabled for notification** to send a test e-mail to all users already set to receive notification.
9. Click **Send Test E-mail** to test the e-mail server.

   A message displays whether the server was found. If the server was not found, verify that the server address was entered correctly and that the server is running. If you are using an SMTP mail server, also verify that the SMTP ID and password information was entered correctly.
10. Click **OK** to save your work and close the **E-mail Event Notification Setup** dialog box.

Setting up advanced event filtering

To set up advanced event filtering on the selected events for a user, complete the following steps.

1. Select **SAN > Users**.

   The **Server Users** dialog box displays.
2. Select a user in the **Users** table and click **Edit**.

   The **Edit User** dialog box displays.
3. Select the **E-mail Notification Enable** check box and click the **Filter** link.

   The **Define Filter** dialog box displays.
4. Click **Advanced Filtering**.

   The **Advanced Event Filtering** dialog box displays.
5. Click the **Include Events** tab.

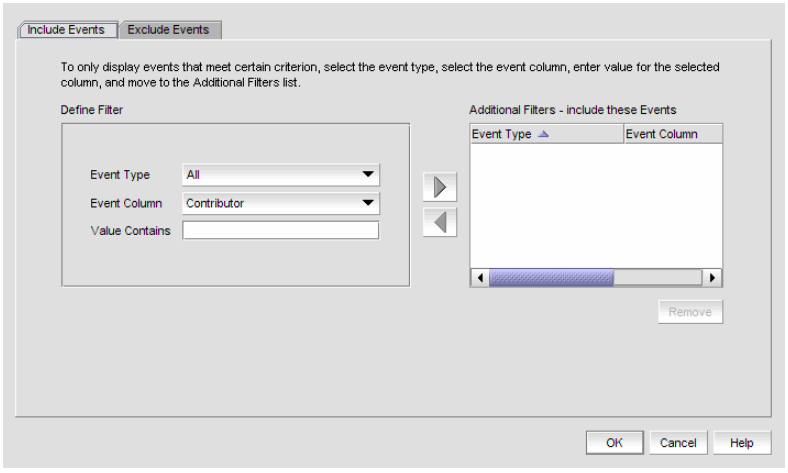


FIGURE 63 Advanced Event Filtering Dialog Box - Include Events tab

   a. Select the event type you want to include from the **Event Type** list.

      All event types are listed in alphabetical order.

b. Select the event column for the event from the **Event Column** list.

   All event columns are listed in alphabetical order.

c. Enter all or part of the event type value in the **Value Contains** text box.

d. Click the right arrow button to move the event type to the **Additional Filters - Filter out these Events** table.

6. Click the **Exclude Events** tab.

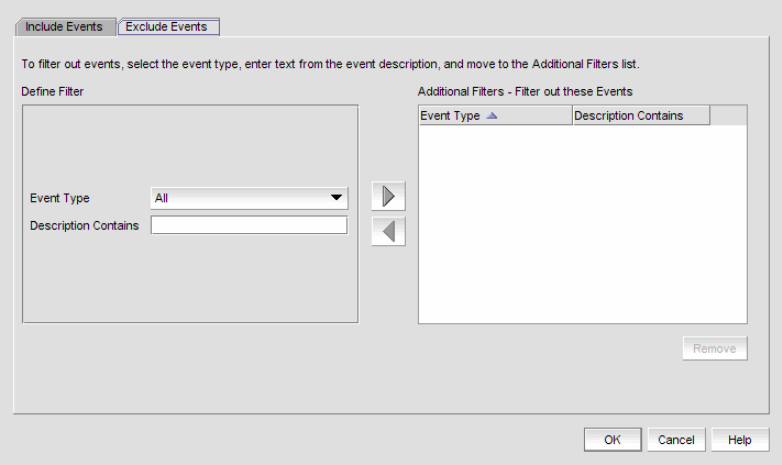


FIGURE 64 Advanced Event Filtering Dialog Box - Include Events tab

a. Select the event type you want to remove from the **Event Type** list.

   All event types are listed in alphabetical order.

b. Enter all or part of the event type description text in the **Description Contains** text box (up to 40 characters).

   This text should be the same text that displayed in the **Description** field for the events that displayed on the Master Log.

c. Click the right arrow button to move the event type to the **Additional Filters - Filter out these Events** table.

7. Click **OK**.

   The **Define Filter** dialog box displays.

8. Click **OK** to close **Define Filter** dialog box.

SNMP trap and informs registration and forwarding

You can configure the application to send SNMP traps and informs to other computers. To correctly configure trap forwarding, you must configure the target computer's IP address and SNMP ports. To correctly configure informs, you must enable informs on the switch.

Registering the management server

NOTE
If the source IP address does not match the switch, the Management application does not forward the SNMP traps.

NOTE
SNMP Informs is only supported on Fabric OS 6.3 or later switches discovered through SNMP v3. For information about discovery through SNMP v3, refer to "Discovering fabrics" on page 39.

You can automatically register this server as the trap or informs recipient on all managed Fabric OS devices.

To register the management server, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.

2. Click the **Management Server** tab.
3. Select the **Auto register server as SNMP trap or informs recipient** check box, if necessary.

   This check box is selected by default.

4. Enter the SNMP listening port number of the Server in the **SNMP Listening Port (Server)** field, if necessary.

   The default SNMP listening port number is 162 and is automatically populated.

5. Click **OK** on the **SNMP Setup** dialog box.

Registering a different Management application server

You can register any Management application server as the trap recipient on managed Fabric OS devices. You can register different recipients for different fabrics.

To register a host server, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.

2. Click the **Other Recipients** tab.
3. Select **Add** from the **Action** list.
4. Enter the IP address (IPv4 or IPv6 format) of the host server in the **Recipient Server IP Address** field.

5. Select a fabric from the **Targeted Fabric** list.
6. Select a severity (None, Critical, Error, Warning, Info, or Debug) from the **Severity** list.
7. Click **OK** on the **SNMP Setup** dialog box.

Removing a host server

You can remove any host server as the trap recipient on managed Fabric OS devices.

To remove a host server, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.
2. Click the **Other Recipients** tab.
3. Select **Remove** from the **Action** list.
4. Click **OK** on the **SNMP Setup** dialog box.

Enabling trap forwarding

You can enable trap forwarding on all defined destinations.

To enable trap forwarding, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.
2. Click the **Trap Forwarding** tab.
3. Select the **Enable trap forwarding** check box.
4. Click **OK** on the **SNMP Setup** dialog box.

Adding an SNMPv1 destination

You can only configure six destinations, including v1 and v3 destinations.

To add a V1 destination, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.
2. Click the **Trap Forwarding** tab.
3. Select **V1** from the **Trap forwarding type** list.

4. Click **Add**.

   The **Add/Edit Trap Recipient** dialog box displays.

   a. (Optional) In the **Description** field, enter a description of the trap recipient.

   b. In the **IP Address** field, enter the trap recipient's IP address.

      The Management application accepts IP addresses in IPv4 or IPv6 formats.

   c. Enter the trap recipient's UDP port number, in the **port** field.

   d. Click **OK** on the **Add/Edit Trap Recipient** dialog box.

5. Click **OK** on the **SNMP Setup** dialog box.

Adding an SNMPv3 destination

You can only configure six destinations, including v1 and v3 destinations.

To add a V3 destination, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.

2. Click the **Trap Forwarding** tab.
3. Select **V3** from the **Trap forwarding type** list.
4. Enter a user name in the **User Name** field.
5. (Optional) Enter a context name in the **Context Name** field.
6. Select the authorization protocol in the **Auth Protocol** field.
7. Enter the authorization password in the **Auth Password** field and the **Retype Password** field.
8. Select the privacy protocol in the **Priv Protocol** field.
9. Enter the privacy password in the **Priv Password** field and the **Retype Password** field.
10. Click **Add**.

    The **Add/Edit Trap Recipient** dialog box displays.

    a. (Optional) In the **Description** field, enter a description of the trap recipient.

    b. In the **IP Address** field, enter the trap recipient's IP address.

       The Management application accepts IP addresses in IPv4 or IPv6 formats.

    c. Enter the trap recipient's UDP port number, in the **port** field.

    d. Click **OK** on the **Add/Edit Trap Recipient** dialog box.

11. Click **OK** on the **SNMP Setup** dialog box.

Editing a destination

To edit a destination, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.

2. Click the **Trap Forwarding** tab.
3. Select the destination you want to edit in the **Destinations** table and click **Edit**.

   The **Add/Edit Trap Recipient** dialog box displays.

   a. (Optional) In the **Description** field, edit the description of the trap recipient.

   b. In the **IP Address** field, edit the trap recipient's IP address.

      The Management application accepts IP addresses in IPv4 or IPv6 formats.

   c. Edit the trap recipient's UDP port number, in the **port** field.

   d. Click **OK** on the **Add/Edit Trap Recipient** dialog box.

4. Click **OK** on the **SNMP Setup** dialog box.

Removing a destination

To remove a destination, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.

2. Click the **Trap Forwarding** tab.
3. Select the destination you want to remove in the **Destinations** table and click **Remove**.

   Press Ctrl and then click to select more than one destination.

4. Click **OK** on the **SNMP Setup** dialog box.

Disabling trap forwarding

You can disable trap forwarding on all defined destinations.

To disable trap forwarding, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.

2. Click the **Trap Forwarding** tab.
3. Clear the **Enable trap forwarding** check box.
4. Click **OK** on the **SNMP Setup** dialog box.

Enabling SNMP informs

NOTE
SNMP Informs is only supported on Fabric OS 6.3 or later switches discovered through SNMP v3. For information about discovery through SNMP v3, refer to "Discovering fabrics" on page 39.

You can enable SNMP informs on all Informs-capable Fabric OS switches.

To enable Informs, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.

2. Click the **Informs** tab.
3. Select the **Enable informs** option.
4. Select the fabric on which you want to enable Informs from the **Fabric** list.

   NOTE
   If you want to enable Informs only on specific switches in a Fabric, you must configure Informs using the Element Manager on each switch or through the command line interface.

   All Informs-capable switches display in the **SNMP Informs Capable Switch in the Fabric** table.

5. Click **OK** on the **SNMP Setup** dialog box.

   SNMP Informs will be enabled on all switches in the **SNMP Informs Capable Switch in the Fabric** table.

Disabling SNMP informs

To disable Informs, complete the following steps.

1. Select **Monitor > SNMP Setup**.

   The **SNMP Setup** dialog box displays.

2. Click the **Informs** tab.
3. Select the **Disable informs** option.
4. Select the fabric on which you want to disable Informs from the **Fabric** list.

   All Informs-capable switches display in the **SNMP Informs Capable Switch in the Fabric** table.

5. Click **OK** on the **SNMP Setup** dialog box.

   SNMP Informs will be disabled on all switches in the **SNMP Informs Capable Switch in the Fabric** table.

Syslog forwarding

NOTE
Syslog messages are only available on Fabric OS devices and Brocade HBAs (managed using HCM Agent).

Syslog forwarding is the process by which you can configure the Management application to send Syslog messages to other computers. Switches only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you must configure the Management application to listen on a different port. Then you must configure another Syslog server to listen for Syslog messages and forward the messages to the Management application Syslog listening port. Brocade HBAs only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you the management application cannot send Syslog messages to another computer.

Syslog messages are persisted in the database. You can view the Syslog messages from the Management application by selecting **Monitor > Log > Syslog**. You can also view audit syslog messages in the Master Log or by selecting **Monitor > Log > Audit Log**.

Registering the management server

You can automatically register this server as the Syslog destination on all managed Fabric OS devices.

NOTE
If the Syslog messages are routed through a relay and the source IP address is not spoofed by the relay before it sends the messages to the Management application, the messages will be dropped.

NOTE
Syslog messages forwarded by the Management application will always use the Management server IP address as the source IP address.

To register the management server, complete the following steps.

1. Select **Monitor > Syslog Configuration**.

   The **Syslog Registration and Forwarding** dialog box displays.

2. Click the **Management Server** tab.
3. Select the **Auto register server as Syslog destination** check box.
4. Enter the Syslog listening port number of the Server in the **Syslog Listening Port (Server)** field.
5. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

Registering a host server

You can register any host server as the Syslog destination on managed Fabric OS devices. You can register different destinations for different fabrics.

To register a host server, complete the following steps.

1. Select **Monitor > Syslog Configuration**.

   The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Other Destination** tab.
3. Select **Add** from the **Action** list.
4. Enter the IP address of the host server in the **Syslog Destination IP Address** field.
5. Select a fabric from the **Targeted Fabric** list.
6. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

Removing a host server

You can remove any host server as the Syslog destination on managed Fabric OS devices.

To remove a host server, complete the following steps.

1. Select **Monitor > Syslog Configuration**.

   The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Other Destination** tab.
3. Select **Remove** from the **Action** list.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

Adding a destination

You can forward Syslog events sent to this server to another destination on a different host.

To add a destination, complete the following steps.

1. Select **Monitor > Syslog Configuration**.

   The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Syslog Forwarding** tab.
3. Click **Add**.

   The **Add/Edit Syslog Recipient** dialog box displays.
   a. (Optional) In the **Description** field, enter a description of the Syslog recipient.
   b. In the **IP Address** field, enter the Syslog recipient's IP address.

      The Management application accepts IP addresses in IPv4 or IPv6 formats.
   c. Enter the Syslog recipient's TCP/IP port number, in the **port** field.
   d. Click **OK** on the **Add/Edit Syslog Recipient** dialog box.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

Editing a destination

To edit a destination, complete the following steps.

1. Select **Monitor > Syslog Configuration**.

   The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Syslog Forwarding** tab.
3. Select the destination you want to edit in the **Destinations** table and click **Edit**.

   The **Add/Edit Syslog Recipient** dialog box displays.
   a. (Optional) In the **Description** field, edit the description of the Syslog recipient.
   b. In the **IP Address** field, edit the Syslog recipient's IP address.

      The Management application accepts IP addresses in IPv4 or IPv6 formats.
   c. Edit the Syslog recipient's TCP/IP port number, in the **port** field.
   d. Click **OK** on the **Add/Edit Syslog Recipient** dialog box.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

Removing a destination

To remove a destination, complete the following steps.

1. Select **Monitor > Syslog Configuration**.

   The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Syslog Forwarding** tab.
3. Select the destination you want to remove in the **Destinations** table and click **Remove**.

   Press Ctrl and then click to select more than one destination.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

Enabling Syslog forwarding

You can enable Syslog forwarding on all defined destinations.

To enable trap forwarding, complete the following steps.

1. Select **Monitor > Syslog Configuration**.

   The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Syslog Forwarding** tab.
3. Select the **Enable Syslog forwarding** check box.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

Disabling Syslog forwarding

You can disable Syslog forwarding on all defined destinations.

To disable Syslog forwarding, complete the following steps.

1. Select **Monitor > Syslog Configuration**.

   The **Syslog Registration and Forwarding** dialog box displays.

2. Click the **Syslog Forwarding** tab.
3. Clear the **Enable Syslog forwarding** check box.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

Chapter

Performance Data

7

In this chapter

- Performance overview 209
- Real-time performance data 215

Performance overview

Performance monitoring provides details about the quantity of traffic and errors a specific port or device generates on the fabric over a specific time frame. You can also use performance to indicate the devices that create the most traffic and to identify the ports that are most congested.

Performance allows you to monitor your SAN by gathering and displaying real-time performance data (FC and GE ports as well as FCIP tunnels).

Performance measures

Performance measures enable you to select one or more measures to define the graph or report. The measures available to you depend on the object type from which you want to gather performance data.

- Tx % Utilization — available for FC, GE, Managed HBA ports, 10GE ports, and FCIP tunnels.
- Rx % Utilization — available for FC, GE, Managed HBA ports, 10GE ports, and FCIP tunnels.
- Tx MB/Sec — available for FC and GE, Managed HBA ports, 10GE ports, FCIP tunnels, and End-to-End monitors.
- Rx MB/Sec — available for FC and GE, Managed HBA ports, 10GE ports, FCIP tunnels, and End-to-End monitors.
- CRC Errors — available for FC, Managed HBA ports, 10GE ports and End-to-End monitors.
- Signal Losses — available for Managed HBA ports and FC ports.
- Sync Losses — available for Managed HBA ports and FC ports.
- Link Failures — available for Managed HBA ports and FC ports.
- Sequence Errors — available for FC ports.
- Invalid Transmissions — available for FC ports.
- Rx Link Resets — available for FC ports.
- Tx Link Resets — available for FC ports.
- Dropped Packets — available for FCIP tunnels only.
- Compression Ratio — available for FCIP tunnels only.
- Latency — available for FCIP tunnels only.
- Link Retransmits — available for FCIP tunnels only.

- Timeout Retransmits — available for FCIP tunnels only.
- Fast Retransmits — available for FCIP tunnels only.
- Duplicate Ack Received — available for FCIP tunnels only.
- Window Size RTT — available for FCIP tunnels only.
- TCP Out of Order Segments — available for FCIP tunnels only.
- Slow Start Status — available for FCIP tunnels only.
- Frames Received — available for 10GE ports only.
- Overflow Errors — available for 10GE ports only.
- Runtime Errors — available for 10GE ports only.
- Receive EOF — available for 10GE ports only.
- Too Long Errors — available for 10GE ports only.
- Underflow Errors — available for 10GE ports only.
- Alignment Errors — available for 10GE ports only.
- NOS Count — available for Managed HBA ports only.
- Error Frames — available for Managed HBA ports only.
- Under Sized Frames — available for Managed HBA ports only.
- Over Sized Frames — available for Managed HBA ports only.
- Primitive Sequence Protocol Errors — available for Managed HBA ports only.
- Dropped Frames — available for Managed HBA ports only.
- Bad EOF Frames — available for Managed HBA ports only.
- Invalid Ordered Sets — available for Managed HBA ports only.
- Non Frame Coding Error — available for Managed HBA ports only.

Performance management requirements

To collect performance data, make sure the following requirements have been met:

- Make sure the snmp access control list for the device is empty or the Management application server IP is in the access control list.

  Example of default access control list

```
FCRRouter:admin> snmpconfig --show accesscontrol
SNMP access list configuration:
Entry 0:  No access host configured yet
Entry 1:  No access host configured yet
Entry 2:  No access host configured yet
Entry 3:  No access host configured yet
Entry 4:  No access host configured yet
Entry 5:  No access host configured yet
```

Example of Management application Server IP included in access control list

```
FCRRouter:admin> snmpconfig --show accesscontrol
SNMP access list configuration:
Entry 0:  Access host subnet area 172.26.1.86 (rw)
Entry 1:  No access host configured yet
Entry 2:  No access host configured yet
Entry 3:  No access host configured yet
Entry 4:  No access host configured yet
Entry 5:  No access host configured yet
```

To add the Management application server IP address to the access control list, use the `snmpconfig --add accesscontrol` command:

To set the default access control, use the `snmpconfig --default accesscontrol` command:

- Make sure that the SNMP credentials in the Management application match the SNMP credentials on the device.
  - To check the SNMP v1 credentials on the device, use the `snmpconfig --show snmpv1` command.

    Example of SNMP v1

    ```
    HCLSwitch:admin> snmpconfig --show snmpv1
    SNMPv1 community and trap recipient configuration:
    Community 1: Secret C0de (rw)
    Trap recipient: 10.103.4.63
    Trap port: 162
    Trap recipient Severity level: 4
    Community 2: OrigEquipMfr (rw)
    Trap recipient: 10.191.12.240
    Trap port: 162
    Trap recipient Severity level: 4
    Community 3: private (rw)
    Trap recipient: 10.103.5.105
    Trap port: 162
    Trap recipient Severity level: 4
    Community 4: public (ro)
    Trap recipient: 192.168.102.41
    Trap port: 162
    Trap recipient Severity level: 4
    Community 5: common (ro)
    Trap recipient: 10.32.150.116
    Trap port: 162
    Trap recipient Severity level: 4
    Community 6: FibreChannel (ro)
    Trap recipient: 1001:0:0:0:0:0:0:172
    Trap port: 162
    Trap recipient Severity level: 4
    ```

- To set the SNMP v1 credentials on the device, use the `snmpconfig --set snmpv1` command.

Example of setting SNMP v1

```
HCLSwitch:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [test]
Trap Recipient's IP address : [172.26.1.183]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [172.26.24.26]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (rw): [custom]
Trap Recipient's IP address : [172.26.1.158]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (ro): [custom]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [172.26.1.145]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
```

- To check the SNMP v3 credentials on the device, use the `snmpconfig --show snmpv3` command.

Example of SNMP v3

```
sw1:FID128:admin> snmpconfig --show snmpv3
SNMPv3 USM configuration:
User 1 (rw): snmpadmin1
Auth Protocol: noAuth
Priv Protocol: noPriv
User 2 (rw): snmpadmin2
Auth Protocol: noAuth
Priv Protocol: noPriv
User 3 (rw): snmpadmin3
Auth Protocol: noAuth
Priv Protocol: noPriv
User 4 (ro): snmpuser1
Auth Protocol: noAuth
Priv Protocol: noPriv
User 5 (ro): snmpuser2
Auth Protocol: noAuth
Priv Protocol: noPriv
User 6 (ro): admin
Auth Protocol: noAuth
Priv Protocol: noPriv
```

- To set the SNMP v3 credentials on the device, use the `snmpconfig --set snmpv3` command.

```
FM_4100_21:admin> snmpconfig --set snmpv3
SNMPv3 user configuration(SNMP users not configured in Fabric OS user
database will have physical AD and admin role as the default):
User (rw): [snmpadmin1] admin
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 1
New Auth Passwd:
Verify Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(1..6) [2] 1
New Priv Passwd:
Verify Priv Passwd:
User (rw): [snmpadmin2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (rw): [snmpadmin3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
SNMPv3 trap recipient configuration:
Trap Recipient's IP address : [192.168.71.32]
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [1.1.1.1]
UserIndex: (1..6) [2]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [10.64.209.171]
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
```

- To check SNMP credentials in the Management application, complete the following steps.

  1. Select **Discover > Setup**.
     The **Discover Setup** dialog box displays.
  2. Select an IP address from the **Available Addresses** table.
  3. Click **Edit**.
     The **Address Properties** dialog box displays.

4. Click the **SNMP** tab.
5. Select the **v1** or **v3** from the **SNMP Version** list.
6. Make sure SNMP credentials match those on the device.
7. Click **OK** on the **Address Properties** dialog box.
8. Click **OK** on the **Discover Setup** dialog box.

- To set SNMP credentials in the Management application, refer to "Configuring SNMP credentials" on page 42.

- Make sure that the SNMP security level is set to the appropriate level for the switch.
  - To check the SNMP security level, use the snmpconfig –show secLevel command.

    Example of checking SNMP security level

    ```
    snmpconfig --show secLevel
    GET security level = 0, SET level = 0
    SNMP GET Security Level: No security
    SNMP SET Security Level: No security
    ```

  - To set the SNMP security level, use the snmpconfig snmpconfig –set secLevel command.

    Example of checking SNMP security level

    ```
    snmpconfig --set secLevel 0
        Select SNMP GET Security Level
        (0 = No security, 1 = Authentication only, 2 = Authentication and Privacy,
        3 = No Access): (0..3) [0]
    ```

- To collect performance for GigE ports and FCIP statistics, make sure that SNMP v3 credentials match (see above) and that FCIP-MIB capability is enabled.
  - To check FCIP-MIB capability, use the `snmpconfig --show mibcapability` command.

    Example of showing FCIP-MIB

    ```
    FCRRouter:admin> snmpconfig --show mibcapability
    FCIP-MIB: YES
    ```

  - To enable FCIP-MIB capability, use the `snmpconfig --set mibcapability` command.

    Example of enabling FCIP-MIB

    ```
    FCRRouter:admin> snmpconfig --set mibcapability
    FA-MIB (yes, y, no, n): [yes]
    FICON-MIB (yes, y, no, n): [yes]
    HA-MIB (yes, y, no, n): [yes]
    FCIP-MIB (yes, y, no, n): [yes]
    ISCSI-MIB (yes, y, no, n): [yes]
    ```

- To collect performance on a Virtual Fabric enabled device, use the `admin> userconfig --show` command to make sure the Fabric OS user has access to all the Virtual Fabrics. Make sure that the SNMPv3 user name is same as the Fabric OS user name. Otherwise, the data is not collected for virtual switches with a non-default VF ID. By default the `admin` user has access to all Virtual Fabrics.

  Example of Fabric OS user verification

  ```
  sw1:FID128:admin> userconfig --show
  Account name: admin
  Description: Administrator
  Enabled: Yes
  Password Last Change Date: Unknown
  Password Expiration Date: Not Applicable
  Locked: No
  Home LF Role: admin
  Role-LF List: admin: 1-128
  Chassis Role: admin
  Home LF: 128
  ```

  - Make sure I/O is running on the switch to obtain real statistics. To view switch statistics, use the `portperfshow <interval>` (FC Ports) or `portshow fciptunnel <Ge port number> <tunnel no> -perf` (FCIP tunnels) command.

  Example for FC ports

  ```
  Sprint-65:root> portperfshow 5
  ```

  Example for FCIP tunnels

  ```
  Sprint-65:root> portshow fciptunnel ge0 1 -perf
  ```

Real-time performance data

Real-time performance enables you to collect data from managed devices in your SAN. Real-time performance is only supported on the following managed objects: FC (E_ and F_ports), GE_ports, 10GE_ports, Managed HBA Ports, and FCIP tunnels. You can use real-time performance to configure the following options:

- Select the polling rate from 10 seconds up to 1 minute.
- Select up to 32 ports total from a maximum of 10 devices for graphing performance.

NOTE
Virtual Fabric logical ISL ports are not included in performance collection.

- Choose to display the same Y-axis range for both the Tx MB/Sec and Rx MB/Sec measure types for easier comparison of graphs.

Generating a real-time performance graph

You can monitor a device's performance through a performance graph that displays transmit and receive data. The graphs can be sorted by the column headers. You can create multiple real-time performance graph instances.

NOTE
To make sure that statistic collection for a switch does not fail, you must configure SNMP credentials for the switch. For step-by-step instructions, refer to "Configuring SNMP credentials" on page 42.

To generate a real-time performance graph for a device, complete the following steps.

1. Select the fabric, device, or port for which you want to generate a performance graph.
2. Choose one of the following options:
   - Select **Monitor > Performance > Real-Time Graph**.

     OR
   - Right-click the device or fabric and select **Performance > Real-Time Graph**.

   If you selected a port, the **Real Time Performance Graphs** dialog box for the selected port displays. To filter real-time performance data from the **Real Time Performance Graphs** dialog box, refer to "Filtering real-time performance data" on page 217.

   If you selected a fabric or device, the **Realtime Port Selector** dialog box displays. Continue with step 3.

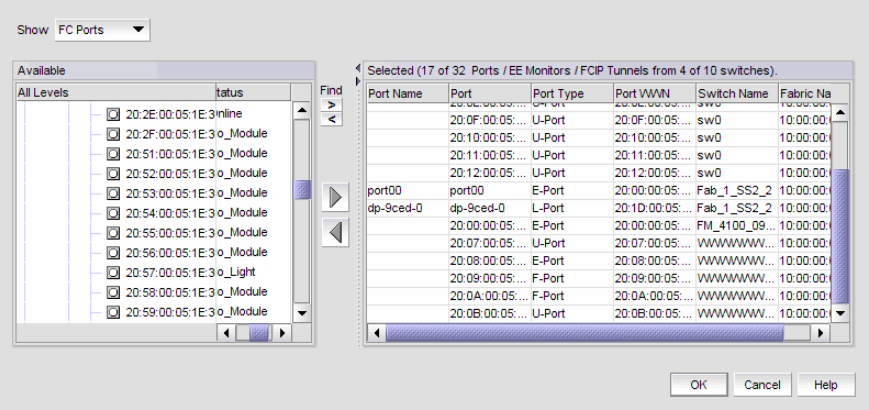


FIGURE 65 Realtime Port Selector dialog box

3. Select the object type (FC Ports, ISL Ports, Device Ports, EE Monitors, GE Ports, FCIP Tunnels, Managed HBA Ports, 10GE Ports) by which you want to graph performance from the **Show** list.
4. Right-click anywhere in the **Available** table and select **Expand All**.
5. Select the ports you want to include in the performance graph in the **Available** table.

   Press **Ctrl** or **Shift** and then click to select more than one port.
6. Click the right arrow to move the selected ports to the **Selected** table.
7. Click **OK**.

   The **Real Time Performance Graphs** dialog box displays.

Filtering real-time performance data

To filter real-time performance data from the **Real Time Performance Graphs** dialog box, complete the following steps.

1. Open the **Real Time Performance Graphs** dialog box.

   For step-by-step instructions, refer to "Generating a real-time performance graph" on page 216. The **Real Time Performance Graphs** dialog box displays.

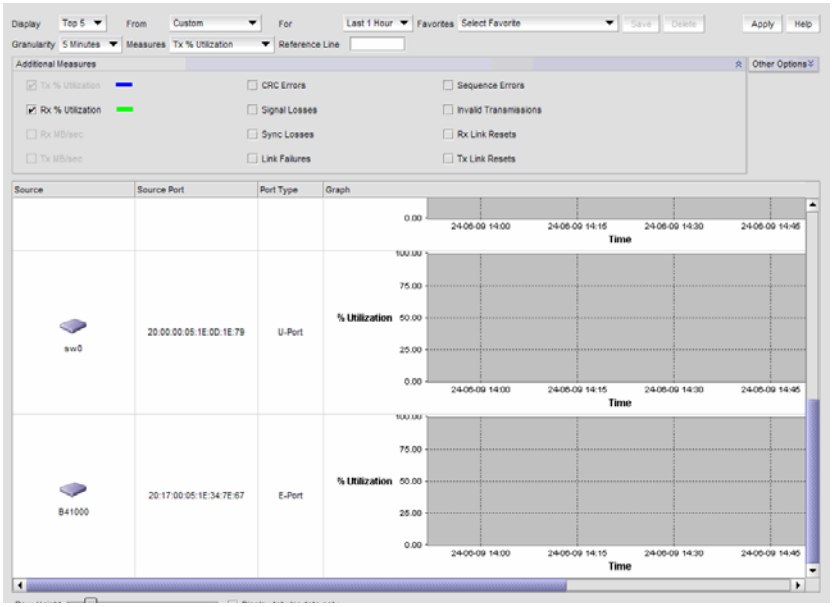


FIGURE 66 **Real Time Performance Graphs dialog box**

2. Click **Select** to change the object type.
3. Select the object type (FC Ports, ISL Ports, Device Ports, EE Monitors, GE Ports, FCIP Tunnels, Managed HBA Ports, 10GE Ports) by which you want to graph performance from the **Show** list.
4. Right-click anywhere in the **Available** table and select **Expand All**.
5. Select the ports you want to include in the performance graph in the **Available** table.

   Press **Ctrl** or **Shift** and then click to select more than one port.
6. Click the right arrow to move the selected ports to the **Selected** table.
7. Click **OK**.

   The **Real Time Performance Graphs** dialog box displays.
8. Select the measure by which you want to gather performance data from the **Measures** list.

   To select more than one measure, click the **Additional Measures** expand arrows and select the check box for each additional measure.
9. (Optional) Enter a value (percentage) in the **Reference Line** field to set a reference for the transmit and receive utilization.

   Note that this field is only available when you select **Tx % Utilization** or **Rx % Utilization** from the **Measures** list.

10. Select the granularity at which you want to gather performance data from the **Granularity** list.
11. Select the **Interpolate** check box to use interpolation to fill existing gaps, if necessary.
12. (Optional) Click **Other Options** and select the **Use Same Y-axis** check box to make the Y-axis range the same for object.

    The **Use Same Y-axis** check box is only available when you select **Rx MB/sec** and **Tx MB/sec** from the **Measures** list. You do not have to apply this change, the performance graph automatically updates.
13. Move the **Row Height** slider to the left to make the row height smaller or to the right to make it bigger.
14. Select the **Display tabular data only** check box to only show text with no graphs or icons.

    The **Source** and **Destination** icons and the **Graph** column do not display
15. Click **Apply**.

    The selected graph automatically displays in the **Real Time Performance Graphs** dialog box.
16. Click the close button (X) to close the **Real Time Performance Graphs** dialog box.

Exporting real-time performance data

To export real-time performance data, complete the following steps.

1. Generate a performance graph.

   To generate a performance graph, refer to "Generating a real-time performance graph" on page 216.
2. Right-click anywhere in the graph table and select **Export Table**.

   The **Save table to a tab delimited file** dialog box displays.
3. Browse to the file location where you want to save the performance data.
4. Enter a name for the file and click **Save**.

Clearing port counters

To reset all port statistic counters to zero on a selected device, complete the following steps.

1. Right-click a device on the Connectivity Map or Product List and select **Performance > Clear Counters**.
2. Click **Yes** on the message.

   A **Port Stats Counter Reset** message displays. If any of the counters do not clear, the message displays a list of the associated ports.
3. Click **Ok** on the **Port Stats Counter Reset** message.

Chapter

8

Reports

In this chapter

- Report types 219
- Generating reports 220
- Viewing reports 220
- Exporting reports 221
- Printing reports 221
- Deleting reports 222
- Generating zoning reports 222

Report types

Presenting and archiving data about a SAN is equally as important as gathering the data. Through the Management application, you can generate reports about the SAN. You can send the reports to network administrators, support consultants, and others interested in the SAN's architecture, or archive them for future reference.

The following standard report types are available from the **Generate Reports** dialog box:

- **Fabric Ports.** Lists discovered ports including used and unused ports. Port data for each fabric is divided into three parts: Fabric-wide port details, Switch-wide port details, and individual port details.
- **Fabric Summary.** Lists information about discovered fabrics including fabric and switch details, device information, and ISL and trunk summary.

The following device specific report is available through the Monitor menu and right-click menus:

- **Zone**. Lists zoning objects.

Generating reports

To generate reports, complete the following steps.

1. Select **Monitor > Reports > Generate**.

   The **Generate Reports** dialog box displays.

2. Select the types of reports you want to generate.

   - Fabric Ports
   - Fabric Summary

3. Select the fabrics for which you want to generate reports.
4. Click **OK**.

   The generated reports display in the **View Reports** dialog box.

   NOTE
   Hyperlinks in reports are active only as long as the source data is available.

5. Click **Close** to close the **View Reports** dialog box.
6. Click **Yes** on the "are you sure you want to close" message.

Viewing reports

You can view any report generated in the SAN. To view reports, complete the following steps.

1. Select **Monitor > Reports > View** or click the **View Report** icon.

   The **View Reports** dialog box displays.

2. Select the report you want to view in the **All Reports** list.

   If you do not see the report you want to view, generate it first by following the instructions in "Generating reports" on page 220.

   You can select reports by Time, Report Type, or User.

3. Use the buttons in the table below to navigate through and resize the report.
4. Click **Show in Browser** to view the selected report in your default browser window.
5. Click **Close** to close the **View Reports** dialog box.
6. Click **Yes** on the "are you sure you want to close" message.

Exporting reports

To export reports, complete the following steps.

1. Select **Monitor > Reports > View** or click the **View Report** icon.

   The **View Reports** dialog box displays.

2. Select the report you want to export in the **All Reports** list.

   If you do not see the report you want to export, generate it first by following the instructions in "Generating reports" on page 220.

   You can select reports by Time, Report Type, or User.

3. Select the format (**PDF**, **HTML**, or **XML**) you want to export to from the list to the left of the **Export** button.

4. Click **Export**.

   The **Save** dialog box displays.

5. Browse to the file location where you want to save the report and click **Save**.

6. Click **Close** to close the **View Reports** dialog box.

7. Click **Yes** on the "are you sure you want to close" message.

Printing reports

You can print reports through an internet browser.

1. Select **Monitor > Reports > View**.

   The **View Reports** dialog box displays.

2. Select the report you want to print in the left pane of the dialog box.

   If you do not see the report you want to view, generate it first by following the instructions in "Generating reports" on page 220.

   NOTE
   Hyperlinks in reports are active only as long as the source data is available.

3. Click **Show in Browser**.

   The selected report displays in your default Web browser.

4. Select **File > Print** (in the Web browser).

   The **Print** dialog box displays.

5. Select the printer to which you want to print and click **Print**.

6. Close the Web browser.

7. Click **Close** in the **View Reports** dialog box.

8. Click **Yes** on the "are you sure you want to close" message.

Deleting reports

To delete reports, complete the following steps.

1. Select **Monitor > Reports > View** or click the **View Report** icon.

   The **View Reports** dialog box displays.

2. Select the report you want to delete in the **All Reports** list.

   If you do not see the report you want to view, generate it first by following the instructions in "Generating reports" on page 220.

   You can select reports by Time, Report Type, or User.

3. Click **Delete Report**.

   ATTENTION
   Once you click **Delete Report**, the report is deleted without confirmation.

4. Click **Close** to close the **View Reports** dialog box.
5. Click **Yes** on the "are you sure you want to close" message.

Generating zoning reports

The Management application enables you to generate a report for the current zone DB in the fabric. To generate a report for the edited zone DB, you must save it to the fabric first. Make sure no one else is making changes to the same area prior to submitting or your changes may be lost.

To generate zoning reports, complete the following steps.

1. Select **Configure > Zoning** or right -click the device and select **Zoning**.

   The **Zoning** dialog box displays.

2. Click **Report**.
3. Click **OK** on the message.

   The selected report automatically displays in the **View Reports** dialog box.

   NOTE
   Hyperlinks in reports are active only as long as the source data is available.

   To print the selected report, refer to "Printing reports" on page 221.

   To export the selected report, refer to "Exporting reports" on page 221.

   To delete the selected report, refer to "Deleting reports" on page 222.

4. Click **Close** to close the **View Reports** dialog box.
5. Click **Yes** on the "are you sure you want to close" message.

   For more information about zoning, refer to "Zoning" on page 377.

Chapter

9

Host management

In this chapter

- About host management 223
- Host discovery 224
- Connectivity map 224
- HBA server mapping 225
- Host performance management 226
- Host fault management 227
- Host Connectivity Manager 228
- Host security authentication 230
- supportSave 232

About host management

Extensive management operations are supported on the switches and fabrics of the SAN using the Management application. Adapters and hosts are visible as part of the fabrics managed by the Management application. The management operations that are currently available using the Management application are discussed in this chapter.

The Management application integrates with another manageability application called the Host Connectivity Manager (HCM) to provide complete management of the host bus adapters (HBAs) and converged network adapters (CNAs).

- The Management application focuses on operations such as fault management, performance management, and configuration management for multiple adapters and adapter ports and security configuration using Fibre Channel Security Protocol (FC-SP) that is set up on the adapter port and the switch.
- HCM supports management for individual adapters (1/4/8 Gbps HBAs) and 10 Gbps CNAs and other devices, such as the host, CEE ports, FCoE ports, and Ethernet ports.

The Management application, in conjunction with HCM, provides end-to-end management capability. For information about configuring, monitoring, and managing individual adapters using the HCM GUI or the Brocade Command Utility (BCU), refer to the *Brocade Adapters Administrator's Guide*.

Host discovery

The Management application enables you to discover individual hosts, import a group of hosts from a CSV file, or import host names from discovered fabrics. The maximum number of host discovery requests that can be accepted is 1000.

NOTE
Host discovery requires HCM Agent 2.0 or later. SMI and WMI discovery are not supported.

Instructions for discovering hosts are detailed in Chapter 2, "Discovery" and include information about the following:

Discovering Hosts by IP address or hostname

Importing Hosts from a CSV file

Importing Hosts from a Fabric

Configuring Brocade HBA credentials

Configuring virtual machine credentials

Editing Host credentials

Removing a Host from Discovery

Viewing the discovery state

Troubleshooting discovery

Connectivity map

The Connectivity Map, which displays in the upper right area of the main widow, is a grouped map that shows physical and logical connectivity of SAN components, including discovered and monitored devices and connections. These components display as icons in the Connectivity Map. For a list of icons that display in the Connectivity Map, refer to the following tables in Chapter 1, "User interface overview":

- "Product icons" on page 16
- "Group icons" on page 17
- "Port icons" on page 17

The Management application displays all discovered fabrics in the Connectivity Map by default. To display a discovered Host in the Connectivity Map, you must select the Host in the Product List. You can only view one Host and physical and logical connections at a time.

HBA server mapping

HBAs and servers discovered through one or more fabrics can be easily identified in the topology by their product icons. For a list of products and their icons, refer to "Product icons" on page 16. Once identified in the topology, you can create servers and assign the HBAs to them and import an externally created HBA server mapping file (.CSV) to the Management application.

NOTE
The Management application now enables you to map HBAs from multiple fabrics (previous versions limited HBA mapping to one fabric).

The Management application also enables you to discover hosts directly using Host discovery (for step-by-step instructions, refer to "Host discovery" on page 44). If you discover a host directly, when you open the **HBA Server Mapping** dialog box the Management application automatically groups all HBAs under the host.

If you create a new HBA server and associate HBAs to it, and then you try to discover a host with the same HBAs using Host discovery, the HBA's discovered using host discovery must match the HBAs associated to the HBA server exactly; otherwise, Host discovery will fail.

Instructions for mapping an HBA server to HBAs are detailed in HBA server mapping in Chapter 5, "Device Configuration" and include information about the following:

- Creating a new HBA server
- Renaming an HBA server
- Deleting an HBA server
- Viewing Server properties
- Associating an HBA with an HBA server
- Importing HBA-to-server mapping
- Removing an HBA from a HBA server

Host performance management

Real-time performance enables you to collect data from managed HBA ports. You can use real-time performance to configure the following options:

- Select the polling rate from 10 seconds up to 1 minute.
- Select up to 32 ports total from a maximum of 10 devices for graphing performance.
- Choose to display the same Y-axis range for both the Tx MB/Sec and Rx MB/Sec measure types for easier comparison of graphs.

Table 26 lists the counters that are supported for the FC ports and for the HBA ports.

TABLE 26

FC port measures	HBA port measures
Tx % utilization	Tx % utilization
Rx % utilization	Rx % utilization
Tx MBps	Tx MBps
Rx MBps	Rx MBps
CRC errors	CRC errors
Signal losses	Signal losses
Sync losses	Sync losses
Link failures	Link failures
Sequence errors	Primitive sequence protocol errors
Invalid transmissions	
Rx link resets	
Tx link resets	
	NOS count
	Error frames
	Dropped frames
	Undersized frames
	Oversized frames
	Bad EOF frames
	Invalid ordered sets
	Non-frame coding error

Instructions for generating real-time performance data are detailed in Generating a real-time performance graph.

Host fault management

Fault management enables you to monitor your SAN using the following methods:

- Monitor logs for specified conditions and notify you or run a script when the specified condition is met.
- Create event-based policies, which contain an event trigger and action.
- Configure E-mail event notification.
- Receive and forward Syslog messages from Fabric OS switches and Brocade HBAs, managed using the Host Connectivity Manager (HCM).

HBA events

You can configure triggers and actions for the following event types that are:

- Product Audit Event — occurs when a target product is audited.
- Product Status Event — occurs when a device or connection changes to Up or Down.
- Product Threshold Alert Event — notifies you when a threshold alert has been reached.

You can configure event policies for events you want to monitor. A policy is the mechanism defined by you that identifies the response to specific event types. You can customize the event management policy using triggers and actions, which are explained in Chapter 6, “Fault Management”.

Event policies

You can create policies for events you want to monitor. A policy is the mechanism defined by you that identifies the response to specific event types. You can customize the event management policy using triggers and actions, which are explained “Event policies” on page 179. This section also provides information about the following topics:

Filtering event notifications

The application provides notification of many different types of SAN events. If a user wants to receive notification of certain events, you can filter the events specifically for that user.

NOTE
The e-mail filter in the Management application is overridden by the firmware e-mail filter. When the firmware determines that certain events do not receive e-mail notification, an e-mail is not sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box.

To configure event notifications, use the instructions in “Configuring e-mail notification” on page 196.

Syslog forwarding

NOTE
Syslog messages are only available on Fabric OS devices and Brocade HBAs (managed using the HCM Agent).

Syslog forwarding is the process by which you can configure the Management application to send Syslog messages to other computers. Switches only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you must configure the Management application to listen on a different port. Then you must configure another Syslog server to listen for Syslog messages and forward the messages to the Management application Syslog listening port. Brocade HBAs only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you the management application cannot send Syslog messages to another computer.

Syslog messages are persisted in the database. You can view the Syslog messages from the Management application. However, the Management application does not convert the Syslog messages into event objects except for the audit syslog messages.

For more information about Syslog forwarding, refer to "Syslog forwarding" on page 204.

Host Connectivity Manager

The Host Connectivity Manager (HCM) is a management software application for configuring, monitoring, and troubleshooting Brocade HBAs and Converged Network Adapters (CNAs) in a storage area network (SAN) environment.

The management software has two components:

- The agent, which runs on the host.
- The management console, which is the graphical user interface client used to manage the HBA or CNA.

You can manage the software on the host or remotely from another host. The communication between the management console and the agent is managed using JSON-RPC over https.

HCM features

Common HBA and CNA management software features include the following:

- Discovery using the agent software running on the servers attached to the SAN, which enables you to contact the devices in your SAN.
- Configuration management, which enables you to configure local and remote systems. With HCM you can configure the following items:
  - Local host
  - Brocade 4 Gbps and 8 Gbps HBAs
  - HBA ports (including logical ports, base ports, remote ports, and virtual ports)
  - Brocade 10 Gbps single-port and 10 Gbps dual-port converged network adapters (CNAs)

  - CEE ports
  - FCoE ports (CNA only)
  - Ethernet ports (CNA only)
- Diagnostics, which enables you to test the adapters and the devices to which they are connected:
  - Link status of each adapter and its attached devices
  - Loopback test, which is external to the adapter, to evaluate the ports (transmit and receive transceivers) and the error rate on the adapter
  - Read/write buffer test, which tests the link between the adapter and its devices
  - FC protocol tests, including echo, ping, and traceroute
- Monitoring, which provides statistics for the SAN components.
- Security, which enables you to specify a CHAP secret and configure authentication parameters.
- Event notifications, which provide asynchronous notification of various conditions and problems through a user-defined event filter.

Launching HCM

Use the Brocade Host Connectivity Manager (HCM) GUI or the Brocade Command Utility (BCU) to enable and manage Brocade adapters. You can open HCM directly from the application.

You must have Device Administration privileges for the selected device to launch HCM. If you do not have Device Administration privileges, you will need to enter those credentials to launch HCM.

To launch HCM, complete the following steps.

On the Connectivity Map, right-click on a Brocade HBA and select **Element Manager**.

HCM Agent displays.

OR

1. Select a Brocade HBA.
2. Select **Configure > Element Manager**.

   The Host Connectivity Manager GUI displays.

For more information about the HCM and BCU commands, refer to the HCM online help or the *Brocade Adapters Administrator's Guide.* For more information about Brocade HBAs, refer to the documentation for the specific device.

Host security authentication

Fibre Channel Security Protocol (FC-SP) is a mechanism used to secure communication between two switches or between a switch and a device such as an HBA port.

You can use either the the Management application or the HCM GUI to display the authentication settings and status. When you enable FC-SP authentication using the Management application, you can also set the authentication settings on the attached 8 Gbps 16-FC-ports, 10 GbE 8-Ethernet Port switch.

NOTE
FC-SP is only available for Brocade HBAs that are managed using the HCM agent. FC-SP is not available for virtual ports or unmanaged HBA ports. The user must have the Security privilege to use this feature.

Configuring security authentication using the Management application

Access the **Fibre Channel Security Protocol Configuration** (FCSP) dialog box by selecting an adapter port from the device tree.

1. Select the appropriate device based on how you want to configure security authentication:
2. Select **Configure > FC-SP** from the main menu right-click the adapter from the list.

   The **Fibre Channel Security Protocol Configuration** (adapter level) dialog box displays. The **Fibre Channel Security Protocol Configuration** dialog at the host level displays.

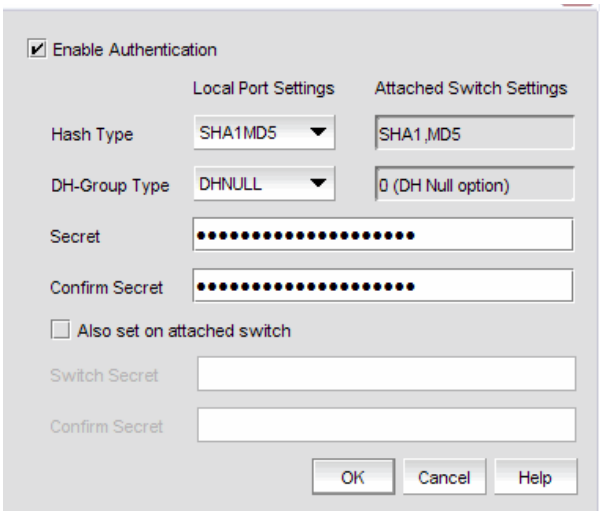


FIGURE 67 Fibre Channel Security Protocol Configuration - host level dialog box

3. Configure the following parameters on the **FCSP Authentication** dialog box:
    a. Select the **Enable Authentication** check box to enable or disable the authentication policy.

       If authentication is enabled, the port attempts to negotiate with the switch. If the switch does not participate in the authentication process, the port skips the authentication process.

       The Hash type list shows the following options, but only one option, DHNULL, is supported.

       - **MD5** - A hashing algorithm that verifies a message's integrity using Message Digest version 5. MD5 produces a 128-bit digest and is the required authentication mechanism for LDAP v3 servers.
       - **SHA1** - A secure hashing algorithm that computes a 160-bit message digest for a data file that is provided as input.
       - **MD5SH1** - Similar to the MD5 hashing algorithm, but used for DH-CHAP authentication.
       - **SHA1MD5** - Similar to the SHA1 hashing algorithm, but used for DH-CHAP authentication.

    b. Select **DHNULL** as the DH-group type value.
    c. Type and retype the secret.

       The length of the secret must be between eight and 41 characters and the secret field cannot be blank.

    d. Click **Apply** to apply the changes.
    e. Select the **Also set on attached switch** check box to enable or disable the authentication policy on the attached switch.
    f. Type and retype the switch secret on the attached switch.

       The maximum length of the switch secret is 63 bytes. The default secret for each interface is its port world wide name (PWWN) without the colons; for example, `0102030405060708`.

    g. Click **Apply** to apply the changes.
4. Click **OK** to save the changes and close the dialog box.

supportSave

Host management features support capturing support information for managed Brocade adapters, which are discovered in the Management application. You can trigger SupportSave for multiple adapters at the same time.

You can use Technical Support to collect supportSave data (such as, RASLOG, TRACE and so on) and switch events from Fabric OS devices.

You can gather technical data for M-EOS devices using the device's Element Manager.

NOTE
The switch must be running Fabric OS 5.2.X or later to collect technical support data. In addition, you must have the supportSave privilege to collect supportSave information.

Instructions for scheduling and capturing technical support files are detailed in "Device Technical Support" on page 164.

Chapter

10

Fibre Channel over IP

In this chapter

- FCIP services licensing 234
- FCIP Concepts 234
- IP network considerations. 234
- FCIP trunking overview 237
- FCIP platforms and supported features. 235
- FCIP trunking overview 237
- IPSec implementation over FCIP 239
- Open systems tape pipelining. 240
- FCIP configuration guidelines. 242
- Configuring an FCIP tunnel 245
- Adding an FCIP circuit 247
- Configuring FCIP Circuit Advanced Settings 248
- Configuring FCIP tunnel advanced settings. 249
- Viewing FCIP connection properties. 253
- Viewing General FCIP properties 254
- Viewing FCIP FC port properties 255
- Viewing FCIP Ethernet port properties 256
- Editing FCIP tunnels 257
- Editing FCIP circuits. 258
- Disabling FCIP tunnels 259
- Enabling FCIP tunnels 259
- Deleting FCIP tunnels 260
- Displaying FCIP performance graphs for FC ports 261
- Displaying FCIP performance graphs for Ethernet ports 261
- Displaying link details for FCIP tunnels 261
- Displaying tunnel properties from the FCIP tunnels dialog box 262
- Displaying FCIP circuit properties from the FCIP tunnels dialog box 263
- Displaying switch properties from the FCIP Tunnels dialog box 264
- Displaying fabric properties from the FCIP Tunnels dialog box 265
- Troubleshooting FCIP Ethernet connections 266

FCIP services licensing

Most of the FCIP extension services described in this chapter require the High Performance Extension over FCIP/FC license. FICON emulation features require additional licenses. Use the **licenseShow** command to verify the needed licenses are present on the hardware used on both ends the FCIP tunnel.

FCIP Concepts

Fibre Channel over IP (FCIP) is a tunneling protocol that enables you to connect Fibre Channel SANs over IP-based networks. Fabric OS extension switches and extension blades use FCIP to encapsulate Fibre Channel frames within IP frames that can be sent over an IP network to a partner Fabric OS extension switch or extension blade. When the IP packets are received, the Fibre Channel frames are reconstructed. FCIP uses a TCP transport that guarantees in-order delivery. The Fibre Channel fabric and all Fibre Channel targets and initiators are unaware of the presence of the IP network.

Because an FCIP tunnel uses an existing IP network, configuring and managing an FCIP tunnel requires knowledge of general IP networking concepts, and specific knowledge about the IP network that will be used for the tunnel. Because the IP network may be used to transport data over very long distances, and because the IP network is not designed exclusively for large data transfers, latency is an issue. Features such as data compression, trunking, Adaptive Rate Limiting (ARL), and Open Systems Tape Pipelining (OSTP) can reduce latency, and help manage tunnel bandwidth more effectively.

IP network considerations

Because FCIP uses TCP connections over an existing IP network, consult with the IP network administrator to be sure that the network hardware and software equipment operating in the data path can support those connections. Routers and firewalls that are in the data path need to be configured to pass layer 3 protocols 0800 (IP), 0806 (ARP), and 0001 (ICMP). Also, process layer ports for FTP (ports 20 and 21) Telnet (port 23), and SNMP (ports 161 and 162) should be configured on the management IP network to enable support personnel to access and transmit troubleshooting information.

FCIP platforms and supported features

There are five Brocade platforms that support FCIP:

- The 8 Gbps 16-FC ports, 6-Gbps ports extension switch.
- The 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade (384-port Backbone Chassis, 192-port Backbone Chassis).
- The 4 Gbps Extension Switch.
- The 4 Gbps Router, Extension switch.
- The 4 Gbps Router, Extension blade (384-port Backbone Chassis, 192-port Backbone Chassis, Director Chassis).

There are differences in platform capabilities. For example, the 4 Gbps Router, Extension switch, the 4 Gbps Extension Switch and the 4 Gbps Router, Extension blade cannot support FCIP trunking, and some features, such as support for IPSec and IPv6 addresses, are not currently available for the 8 Gbps 16-FC ports, 6-Gbps ports extension switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade in Fabric OS version 6.3.0, but are planned for a later version. Table 27 summarizes FCIP capabilities per platform.

TABLE 27 FCIP capabilities by platform

Capabilities	8 Gbps 16-FC ports, 6-Gbps ports extension switch	8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade	4 Gbps Router, Extension Switch	4 Gbps Router, Extension blade
FCIP trunking	Yes	Yes	No	No
Adaptive Rate Limiting	Yes	Yes	No	No
10 GbE ports	No	Yes	No	No
FC ports up to 8 Gbps	Yes	Yes	No	No
Compression	4:1 and higher	4:1	2:1	2:1
Open Systems Tape Pipelining (OSTP) • FCIP Fastwrite • Tape Acceleration	Yes	Yes	Yes	Yes
Traffic shaping and QoS	Yes	Yes	Yes	Yes
FICON extension	Yes	Yes	Yes	Yes
IPSec for tunnel traffic	No*	No*	Yes	Yes
Diffserv priorities	No*	No*	Yes	Yes
VLAN tagging	No*	No*	Yes	Yes
VEX_Ports	Yes	No	Yes	Yes
Support for third party WAN optimization hardware	No*	No*	Yes	Yes
IPv6 addresses for FCIP tunnels	No*	No*	Yes	Yes

*Not supported in Fabric OS version 6.3.0, but will be supported in a later version.

The way FCIP tunnels and virtual ports map to the physical GbE ports depends on the switch or blade model. The 8 Gbps 16-FC ports, 6-Gbps ports extension switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade tunnels are not tied to a specific GbE port, and may be assigned to any virtual port within the allowed range. The 4 Gbps Router, Extension switch and 4 Gbps Router, Extension blade require tunnels to be mapped to specific GbE ports and specific virtual ports. The mapping of GbE ports to tunnels and virtual port numbers is summarized in Table 28.

TABLE 28 Tunnel and virtual port numbering

Switch or Blade Model	GbE ports	Tunnels	Virtual ports (VE_Ports, VEX_Ports)
8 Gbps 16-FC ports, 6-Gbps ports extension switch	GbE ports 0-5	0-8	16-23
8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade	GbE ports 0-9 10GbE ports 10, 11	0-20	12-23 used by GbE ports (0-9) 24-31 used by 10GbE ports (10, 11) • XGE1 uses VE-Ports 12-21 • XGE0 uses VE-Ports 22-31
4 Gbps Router, Extension switch and blade	ge0	0 1 2 3 4 5 6 7	16 17 18 19 20 21 22 23
	ge1	0 1 2 3 4 5 6 7	24 25 26 27 28 29 30 31

The 4 Gbps Extension Switch presents only 2 active FC ports and 1 virtual port per GbE interface (ge0 and ge1 in the table above).

FCIP trunking overview

FCIP trunking is a method for managing the use of WAN bandwidth. Trunking is enabled by creating logical circuits within an FCIP tunnel. A tunnel may have multiple circuits. Each circuit represents a portion of the available Ethernet bandwidth provided by the GbE ports that are connected to the WAN.

NOTE
FCIP trunking is available only on the 8 Gbps 16-FC ports, 6-Gbps ports extension switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade. The 4 Gbps Router, Extension switch and blade do not support FCIP trunking.

Figure 68 shows the relationship of trunks and circuits to VE_Ports, FCIP tunnels, and the physical GbE interfaces. FC traffic enters and exits an FCIP tunnel on a VE_Port. Applications on the FC side have no awareness of the existence of the FCIP tunnel. FCIP Trunking routes the FC traffic over FCIP circuits. FCIP circuits route traffic over a WAN using any of the GbE interfaces. An FCIP circuit is a logical connection between two peer switches or blades, so the same construct exists in each peer switch or blade.

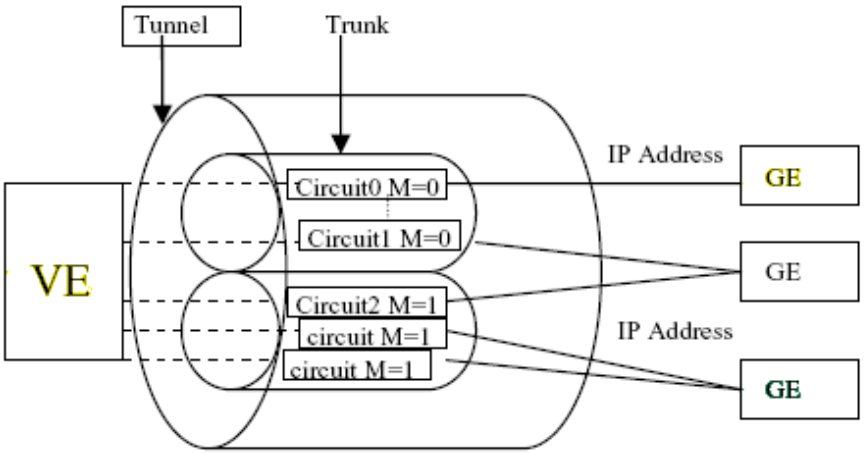


FIGURE 68 **Basic overview of trunking components**

Load leveling and failover using FCIP trunking

Each FCIP circuit is assigned a metric, which is used in managing load leveling and failover for FC traffic. FCIP trunking uses the metric to determine if a circuit is to be used for load leveling or failover. Figure 68 shows five circuits and their assigned metrics (0 or 1). Load leveling is automatically done across circuits with the lowest metric. If a circuit fails, FCIP trunking tries first to retransmit any pending send traffic over another lowest metric circuit. If no lowest metric circuits are available, then the pending send traffic is retransmitted over any available circuits with the higher metric.

Adaptive Rate Limiting and QoS priorities

Each FCIP circuit is assigned four TCP connections for managing FC Quality of Service (QoS) priorities over an FCIP tunnel. The priorities are as follows:

- F class - F class is the highest priority, and is assigned bandwidth as needed, at the expense of lower priorities, if necessary.
- QoS high - The QoS high priority gets at least 50% of the bandwidth.
- QoS medium - The QoS medium priority gets at least 30% of the bandwidth.
- QoS low - The QoS low priority gets at least 20% of the bandwidth.

Adaptive Rate Limiting (ARL) allows you to dynamically adjust bandwidth across priorities so that a single QoS priority may consume the entire bandwidth when no other QoS priority is in use. ARL applies a minimum and maximum traffic rate on a circuit, and allows the traffic demand and WAN connection quality to dynamically determine the rate. As traffic increases, the rate grows towards the maximum rate, and if traffic subsides, the rate reduces towards the minimum. If traffic is flowing error-free over the WAN, the rate grows towards the maximum rate. If TCP reports an increase in retransmissions, the rate reduces towards the minimum.

FCIP Trunk design considerations

There are three basic points to consider when designing an FCIP trunk:

- Each FCIP circuit is assigned a pair of IP addresses, one source IP address, and one destination IP address.
- The source IP address is used to determine which GbE interface to use. The GbE IP address must be on the same IP subnet as the source IP address. IP subnets cannot span across the GbE interfaces.
- The destination IP address is used to determine routing. If the destination IP address is also on the same subnet as the GbE interface, packets are routed over that subnet. If the destination IP address is on a different subnet, it must be routed to an IP gateway address.

IPSec implementation over FCIP

Internet Protocol security (IPsec) uses cryptographic security to ensure private, secure communications over Internet Protocol networks. IPsec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. It helps secure your SAN against network-based attacks from untrusted computers, attacks that can result in the denial-of-service of applications, services, or the network, data corruption, and data and user credential theft. By default, when creating an FCIP tunnel, IPsec is disabled.

Used to provide greater security in tunneling on an 4 Gbps Router, Extension blade or switch, the IPsec feature does not require you to configure separate security for each application that uses TCP/IP. When configuring for IPsec, however, you must ensure that there is an 4 Gbps Router, Extension Blade or a Switch at each end of the FCIP tunnel. IPsec works on FCIP tunnels with or without IP compression (IPComp), FCIP Fastwrite, and tape acceleration. IPsec can only be created on tunnels using IPv4 addressing.

NOTE
Fabric OS version 6.3.0 does not support IPSec for the 8 Gbps 16-FC ports, 6-Gbps ports extension switch or
8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade.

IPsec uses some terms that you should be familiar with before beginning your configuration. These are standard terms, but are included here for your convenience.

TABLE 29 IPsec terminology

Term	Definition
AES	Advanced Encryption Standard. FIPS 197 endorses the Rijndael encryption algorithm as the approved AES for use by US Government organizations and others to protect sensitive information. It replaces DES as the encryption standard.
AES-XCBC	Cipher Block Chaining. A key-dependent one-way hash function (MAC) used with AES in conjunction with the Cipher-Block-Chaining mode of operation, suitable for securing messages of varying lengths, such as IP datagrams.
AH	Authentication Header - like ESP, AH provides data integrity, data source authentication, and protection against replay attacks but does not provide confidentiality.
DES	Data Encryption Standard is the older encryption algorithm that uses a 56-bit key to encrypt blocks of 64-bit plain text. Because of the relatively shorter key length, it is not a secured algorithm and no longer approved for Federal use.
3DES	Triple DES is a more secure variant of DES. It uses three different 56-bit keys to encrypt blocks of 64-bit plain text. The algorithm is FIPS-approved for use by Federal agencies.
ESP	Encapsulating Security Payload is the IPsec protocol that provides confidentiality, data integrity and data source authentication of IP packets, and protection against replay attacks.
IKE	Internet Key Exchange is defined in RFC 2407, RFC 2408 and RFC 2409. IKEv2 is defined in RFC 4306. IKE uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived and communicating parties are authenticated. The IKE protocol creates a security association (SA) for both parties.
MD5	Message Digest 5, like SHA-1, is a popular one-way hash function used for authentication and data integrity.
SHA	Secure Hash Algorithm, like MD5, is a popular one-way hash function used for authentication and data integrity.

TABLE 29 IPsec terminology (Continued)

Term	Definition
MAC	Message Authentication Code is a key-dependent, one-way hash function used for generating and verifying authentication data.
HMAC	A stronger MAC because it is a keyed hash inside a keyed hash.
SA	Security Association is the collection of security parameters and authenticated keys that are negotiated between IPsec peers.

The following limitations apply to using IPsec:

- IPSec is not supported on 10GbE ports.
- IPsec-specific statistics are not supported.
- To change the configuration of a secure tunnel, you must delete the tunnel and recreate it.
- There is no RAS message support for IPsec.
- IPsec can only be configured on IPv4 based tunnels.
- Secure Tunnels cannot be defined with VLAN Tagged connections.
- For the 4 Gbps Router, Extension switch and blade:
  - IPv6, NAT, and AH are not supported.
  - You can only create a single secure tunnel on a port; you cannot create a nonsecure tunnel on the same port as a secure tunnel.
  - Jumbo frames are not supported.

Open systems tape pipelining

Open Systems Tape Pipelining (OSTP) can be used to enhance open systems SCSI tape write I/O performance. To implement OSTP over FCIP, you must enable the following two features:

- FCIP Fastwrite and Tape Acceleration.
- FC Fastwrite.

FCIP Fastwrite and Tape Acceleration

When the FCIP link is the slowest part of the network, consider using FCIP Fastwrite and Tape Read and Write Pipelining. FCIP Fastwrite and Tape Acceleration are two features that provide accelerated speeds for read and write I/O over FCIP tunnels in some configurations:

- FCIP Fastwrite accelerates the SCSI write I/Os over FCIP.
- Tape Acceleration accelerates SCSI read and write I/Os to sequential devices (such as tape drives) over FCIP, which reduces the number of round-trip times needed to complete the I/O over the IP network and speeds up the process. To use Tape Acceleration, you must also enable FCIP Fastwrite.

Both sides of an FCIP tunnel must have matching configurations for these features to work. FCIP Fastwrite and Tape Acceleration are enabled by turning them on during the tunnel configuration process. They are enabled on a per-FCIP tunnel basis.

Consider the constraints described in Table 30 when configuring tunnels to use OSTP.

TABLE 30 Using FCIP Fastwrite and Tape Acceleration

FCIP Fastwrite	Tape Acceleration
Each GbE port supports up to 2048 simultaneous accelerated exchanges, which means *a total of 2048 simultaneous exchanges combined* for Fastwrite and Tape Acceleration.	Each GbE port supports up to 2048 simultaneous accelerated exchanges, which means *a total of 2048 simultaneous exchanges combined* for Fastwrite and Tape Acceleration.
Does not natively support multiple equal-cost path configurations. Traffic isolation zoning can be used to support these configurations.	Does not natively support multiple equal-cost path configurations or multiple non-equal-cost path configurations. . Traffic isolation zoning can be used to support these configurations.
Class 3 traffic is accelerated with Fastwrite.	Class 3 traffic is accelerated between host and sequential device.
	With sequential devices (tape drives), there are 1024 initiator-tape (IT) pairs per GbE port, but 2048 initiator-tape-LUN (ITL) pairs per GbE port. The ITL pairs are shared among the IT pairs. For example: Two ITL pairs for each IT pair as long as the target has two LUNs. If a target has 32 LUNs, 32 ITL pairs for IT pairs. In this case, only 64 IT pairs are associated with ITL pairs. The rest of the IT pairs are not associated to any ITL pairs, so no Tape Acceleration is performed for those pairs. By default, only Fastwrite-based acceleration is performed on the unassociated pairs.
	Does not support multiple non-equal-cost path between host and sequential device

Virtual Port Types

Virtual ports may be defined as VE_Ports.

VE_Ports

VE_Ports (virtual E_Ports) are used to create interswitch links (ISLs) through an FCIP tunnel. If VE_Ports are used on both ends of an FCIP tunnel, the fabrics connected by the tunnel are merged.

FCIP configuration guidelines

FCIP configuration always involves two or more extension switches. The following must take place first before you can successfully configure a working FCIP connection from the Management application:

- The Management application must have management port access to the extension switches.
- The Management application must be able to discover the fabrics the contain the extension switches.
- The extension switches should be physically connected to the IP network they will be using to pass data, and the connection should be active and working. Maximum Transmission rate and MTU size configuration parameters are negotiated over an active connection.
- Identify all the devices in the data path between the extension switches, including Ethernet switches, Ethernet routers, firewalls, and common carrier equipment. A network diagram is very helpful. Support engineers may ask you to provide a network diagram when troubleshooting problems.
- Routers and firewalls must be configured to pass ARP, ICMP, and IP layer 3 protocols.
- Persistently disable the virtual ports before you configure them. Ports on a new extension switch or extension blade are persistently disabled by default. On an extension switch or blade that has already been installed and configured, check the VE_Port status using the portcfgshow command, and persistently disable the ports before you configure them.
- The Ethernet port associated with the tunnel should also be disabled. Disabling the Ethernet port will disable all tunnels on the port. Before disabling an Ethernet port, be sure there are no other tunnels active on the port.
- Determine which features you are implementing, and gather the information needed to implement those features. Table 27 summarizes feature support per FCIP platform.

Additional guidelines for tunnel advanced settings

The following features are implemented as advanced settings on the **Add FCIP Tunnel** dialog box:

- Data compression.
- Open Systems Tape Pipelining (FCIP Fast Write and Tape Acceleration).
- IPSec and IKE settings for cryptographic security over IP networks.
- FICON emulation/acceleration features that improve performance in FICON environments.
- tperf test mode. See the *Fabric OS FCIP Administrator's Guide* for information about tperf.

Data compression

Data compression can improve performance on long distance connections. Compression is enabled by selecting **Advanced Settings** on the **Add FCIP Tunnel** dialog box. Compression options are available on the **Transmission** tab. Compression is done by the hardware. A value of 1 enables compression. For the 4 Gbps Router, Extension switch and blade, the compression ratio is typically 2:1. For the 8 Gbps 16-FC ports, 6-Gbps ports extension switch and the 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade, the compression ratio is typically 4:1. The 8 Gbps 16-FC ports, 6-Gbps ports extension switch provides two additional levels of software compression. Settings 2 and 3 provide incrementally higher compression ratios that can be used to improve performance on slower links. A value of 0 disables compression.

Open systems tape pipelining (OSTP)

Latency introduced by a long distance IP connection can negatively impact tape I/O performance. OSTP may be used to improve performance on SCSI write I/Os to sequential devices (such as tape drives). When OSTP is used, the extension blades or switches emulate write commands and responses locally to reduce delays caused by latency. Both sides of an FCIP tunnel must have matching configurations for these features to work. OSTP may be configured by selecting **Advanced Settings** on the **Add FCIP Tunnel** dialog. OSTP options are available on the **Transmission** tab.

IPSec and IKE policies

IPSec and IKE policy creation is an independent procedure. These policies must be in place before you assign the policies when creating the FCIP tunnel, and you must have them available when you run the **FCIP Tunnel Configuration** wizard. These policies are assigned by selecting **Advanced Settings** on the **Configure Tunnel** dialog. The following limitations apply to using IPSec:

- IPv6, NAT, and AH are not supported.
- You cannot create a nonsecure tunnel on the same port as a secure tunnel.
- IPSec-specific statistics are not supported.
- Jumbo frames are not supported for IPSec.
- There is no RAS message support for IPSec.
- Only a single route is supported on an interface with a secure tunnel.
- Maximum unidirectional throughput is approximately 104 MBps.
- Maximum bidirectional throughput is approximately 104 MBps.

FICON emulation features

FICON emulation supports FICON traffic over IP WANs using FCIP as the underlying protocol. FICON emulation features support performance enhancements for specific applications. If you are using FCIP for distance extension in a FICON environment, evaluate the need for these features before you run the FCIP configuration wizard. FICON emulation may be configured by selecting **Advanced Settings** on the **Configure Tunnel** dialog. The following features are available:

- XRC emulation.
- Tape write pipelining.
- Tape read pipelining.

XRC emulation

The eXtended Remote Copy (XRC) application is a DASD application that implements disk mirroring, as supported by the disk hardware architecture and a host software component called System Data Mover (SDM). The primary volume and the secondary mirrored volume may be geographically distant across an IP WAN. The latency introduced by greater distance creates delays in anticipated responses to certain commands. The FICON pacing mechanism may interpret delays as an indication of a large data transfer that could monopolize a shared resource, and react by throttling the I/O. XRC emulation provides local responses to remote hosts, eliminating distance related delays. A FICON XRC Emulation License is required to enable XRC Emulation.

Tape write pipelining

FICON tape write pipelining improves performance for a variety of applications when writing to tape over extended distances. FICON tape write pipelining locally acknowledges write data records, enabling the host to generate more records while previous records are in transit across the IP WAN. If exception status is received from the device, the writing of data and emulation is terminated. The FICON Tape Emulation License is required to enable FICON Tape Write Pipelining.

Tape read pipelining

FICON tape read pipelining improves performance for certain applications when reading from FICON tape over extended distances. FICON tape read pipelining reads data from tape directly from the tape device. Reading of tape continues until a threshold is reached. The buffered data is forwarded to the host in response to requests from the host. When the host sends the status accept frame indicating that the data was delivered, the read processing on the device side credits the pipeline and requests more data from the tape. If exception status is received from the device, the reading of data and emulation is terminated. The FICON Tape Emulation License is required to enable FICON Tape Read Pipelining.

Configuring an FCIP tunnel

When you configure an FCIP extension connection, you create FCIP tunnels and FCIP circuits, between two extension switches.

1. Select **Configure > FCIP Tunnels**.

   The **FCIP Tunnels** dialog box is displayed (Figure 69). All discovered fabrics with extension switches are listed under devices.

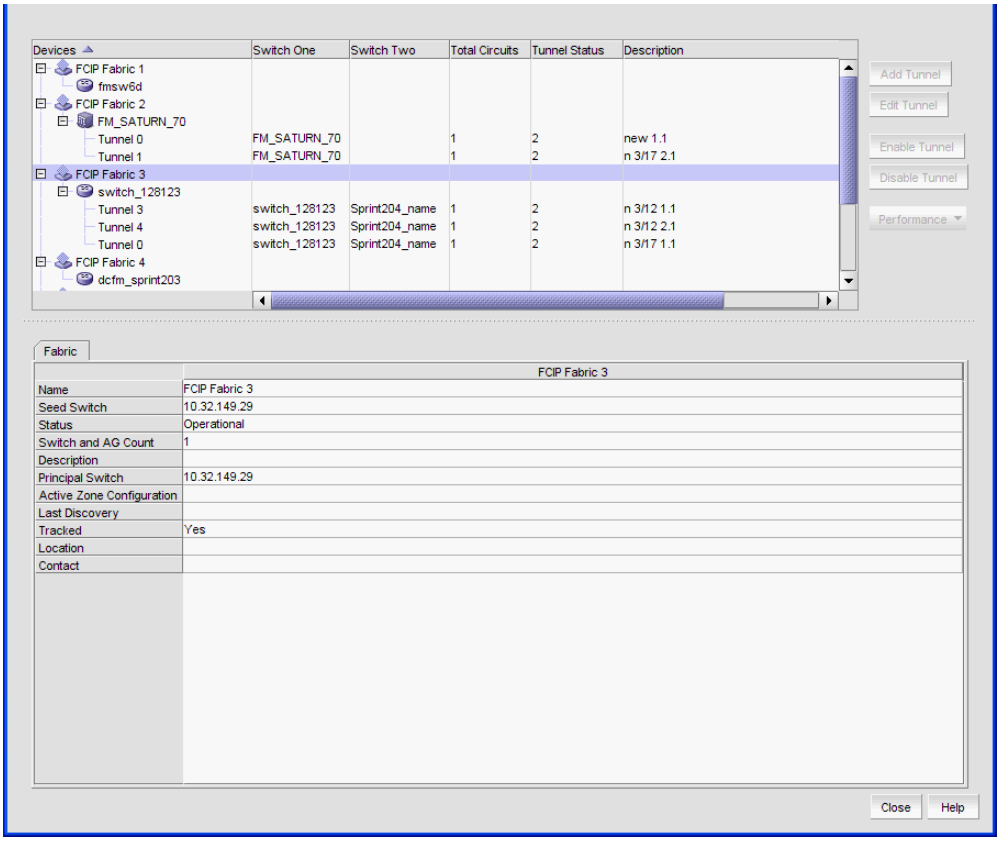
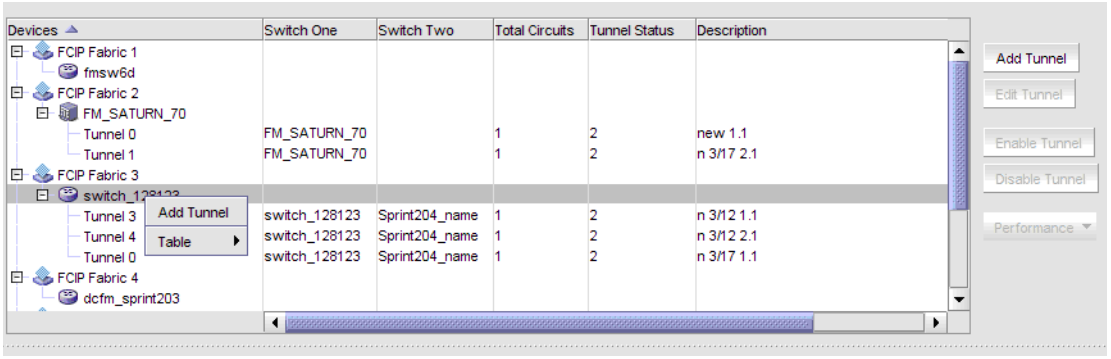


FIGURE 69 **FCIP Tunnels dialog box**

2. Select the switch you want to configure under **Devices**.



3. Click the **Add Tunnel** button, or right-click on the switch and select **Add Tunnel**.

   The **Add FCIP Tunnel** dialog is displayed (Figure 70). The name of the switch you selected is displayed in the **Switch** field under **Switch One Settings**. This dialog allows you to configure settings for both switches on either end of the tunnel.

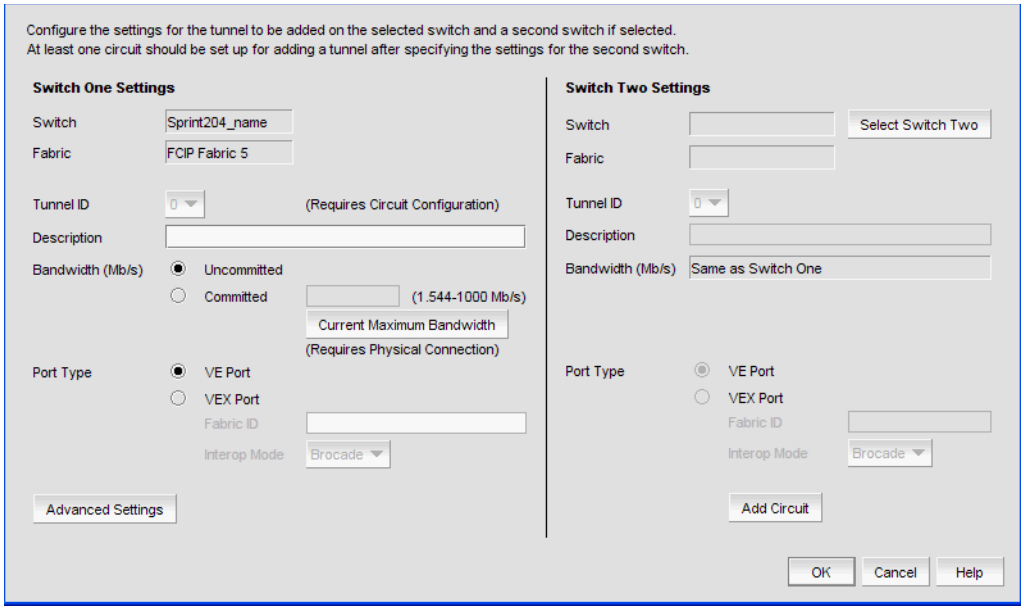


FIGURE 70 Add FCIP Tunnel dialog box

4. Click **Select Switch Two** under **Switch Two Settings** to display discovered extension switches, and select the switch that you want to connect to switch one.

   The switch name and fabric are displayed in the **Switch** and **Fabric** fields.

5. Enter a description of the tunnel in the **Description** field.

NOTE
You cannot assign a **Tunnel ID** until after at least one circuit is configured. The **Add Circuit** dialog returns you to the **Add FCIP Tunnel** dialog to allow you to select the **Tunnel ID**.

6. Select **Add Circuit**.

   The **Add FCIP Circuit** dialog is displayed. Continue with "Adding an FCIP circuit".

Adding an FCIP circuit

FCIP circuits are added by selecting the **Add Circuit** button on the **Add FCIP Tunnel** dialog box. The **Add FCIP Circuit** dialog box is displayed (Figure 71).

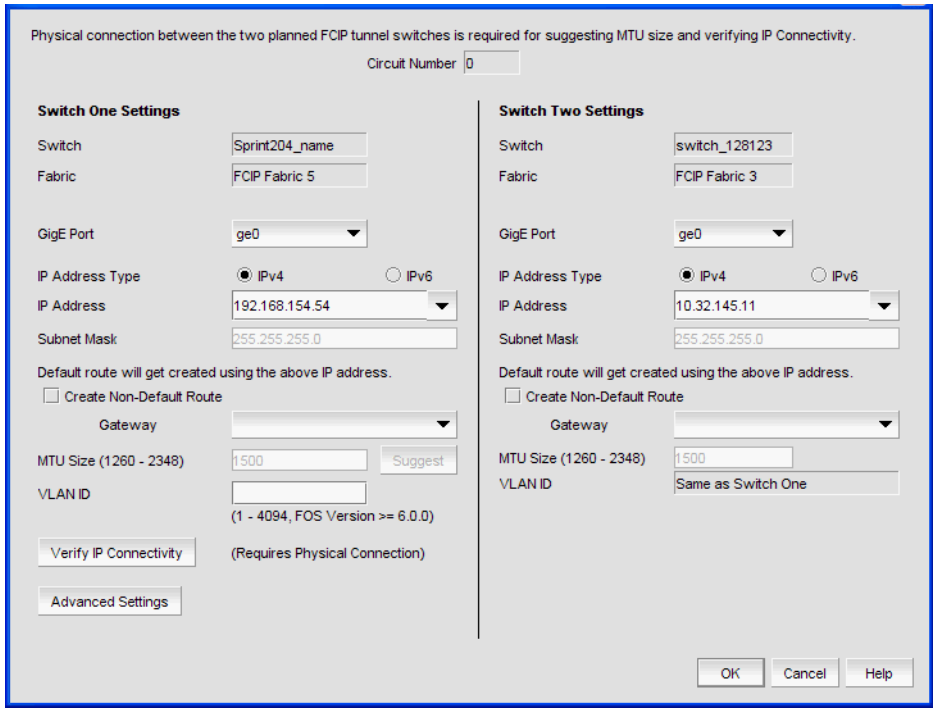

Physical connection between the two planned FCIP tunnel switches is required for suggesting MTU size and verifying IP Connectivity.
Circuit Number 0
Switch One Settings
Switch Sprint204_name
Fabric FCIP Fabric 5
GigE Port ge0
IP Address Type IPv4 IPv6
IP Address 192.168.154.54
Subnet Mask 255.255.255.0
Default route will get created using the above IP address.
Create Non-Default Route
Gateway
MTU Size (1260 - 2348) 1500 Suggest
VLAN ID
(1 - 4094, FOS Version >= 6.0.0)
Verify IP Connectivity
(Requires Physical Connection)
Advanced Settings
Switch Two Settings
Switch switch_128123
Fabric FCIP Fabric 3
GigE Port ge0
IP Address Type IPv4 IPv6
IP Address 10.32.145.11
Subnet Mask 255.255.255.0
Default route will get created using the above IP address.
Create Non-Default Route
Gateway
MTU Size (1260 - 2348) 1500
VLAN ID Same as Switch One
OK
Cancel
Help

FIGURE 71 **Add FCIP Circuit dialog box**

1. Select the **GiGE Port** used for the Ethernet connection on each switch. The choices available depend on the extension switch or blade model.
2. Select the **IP Address Type**. IPv4 and IPv6 address formats cannot be mixed. Addresses must be entered in the same format.
3. Select the **IP Address** for each port.
4. For IPv4 addresses, specify the **Subnet Mask**.

   The default is created from the IP address and Subnet Mask. If you want to create a route through a gateway router, click **Create Non-Default Route**, and select a **Gateway address**.
5. Enter the **MTU Size**.

   For SAN traffic, the largest possible MTU (Maximum Transmission Unit) size is generally the most efficient. If you have an active connection between switch one and switch two, click **Suggest** under **Switch One Settings**. To determine a suggested size, packets are sent across the FCIP tunnel, starting at the largest possible size packet that can be sent over IP. If a valid connection response is not received, a smaller packet is sent. This continues until a valid connection response is received, and that size becomes the suggested MTU. MTU settings must match at both ends of the tunnel, and the setting specified under **Switch One Settings** is automatically applied to switch two.

6. If a VLAN ID is used to route frames between the switches over the physical connection, enter the **VLAN ID** under **Switch One Settings**. The same VLAN ID is automatically assigned to switch two.
7. Select values for bandwidth settings. An uncommitted bandwidth is not allowed on an FCIP circuit. You must select Committed bandwdith, and set **Minimum** and **Maximum** bandwidth values. Bandwidth grows towards the maximum and reduces towards the minimum based on traffic conditions.
8. If the physical connection exists, click **Verify IP Connectivity** to test the connection between switch one and switch two. The IP connectivity of the connection is tested with the ping utility.
9. Select **Advanced Settings** and continue with Configuring FCIP Circuit Advanced Settings if you want to do any of the following.:
   - Turn selective acknowledgement off.
   - Use the circuit as a failover circuit.
   - Set the keep alive timeout to a value other than the default of 10 seconds.
   - Set the minimum retransmission time to a value other than the default of 100 ms.
   - Set the maximum retransmits to a value other than the default.

Configuring FCIP Circuit Advanced Settings

If you select **Advanced Settings**, the **Transmission tab** of the **FCIP Circuit Advanced Settings** dialog box displays.

- Select the **Selective Ack Off** check box to disable selective acknowledgement. Selective acknowledgement is desirable, but some systems may have a requirement to disable selective acknowledgement.
- The **Metric** option is used to identify a failover circuit. By assigning a non-zero metric (1), you identify the circuit as a failover circuit. By default, a circuit is assigned a metric of 0. If a circuit fails, FCIP trunking tries first to retransmit any pending send traffic over another circuit with a metric of 0. If no circuits with a metric of 0 are available, then the pending send traffic is retransmitted over any available circuit with a metric of 1.
- Use the **Keep Alive Time Out (ms)** option to override the default value of 10000 ms. As shown, the range is from 8000 to 7200000.
- Use the **Max. Retransmission Time (ms)** option to override the default value of 100 ms.
- Use **Max. Retransmits** option to override the default value of 8. As shown, the range is 1 to 8.

10. Click **Finish** to close the **FCIP Tunnel Configuration** wizard.

Configuring FCIP tunnel advanced settings

Compression, FCIP fast write and tape pipelining, IPSec and IKE policies, and FICON emulation features are configured as advanced settings.

1. Click **Advanced Settings** on the **Configure Tunnel** dialog box.

   The **Advanced Settings** dialog box is displayed. This dialog box has a **Transmission** tab, **Security** tab, and **FICON Emulation** tab.

2. Click **OK** to close Advanced settings when you have configured the features that you want to implement.

3. Click **Next** to continue.

   A summary of the configuration parameters is shown. A rotating arrow under **Status** indicates a configuration step is in progress. A blue check mark indicates successful completion of all steps for that Configuration Item. A red stop sign indicates a failed step. If the configuration is successful, all configuration items have blue check marks.

   The tunnel configuration begins. You can see a progress bar and the configuration results in the wizard **Report** panel

4. Click **Finish** to close the **FCIP Tunnel Configuration** wizard.

Compression, OSTP, and Tperf

Compression, OSTP (fast write and tape pipelining) and Tperf test mode are enabled from the **Transmissions** tab (Figure 72).

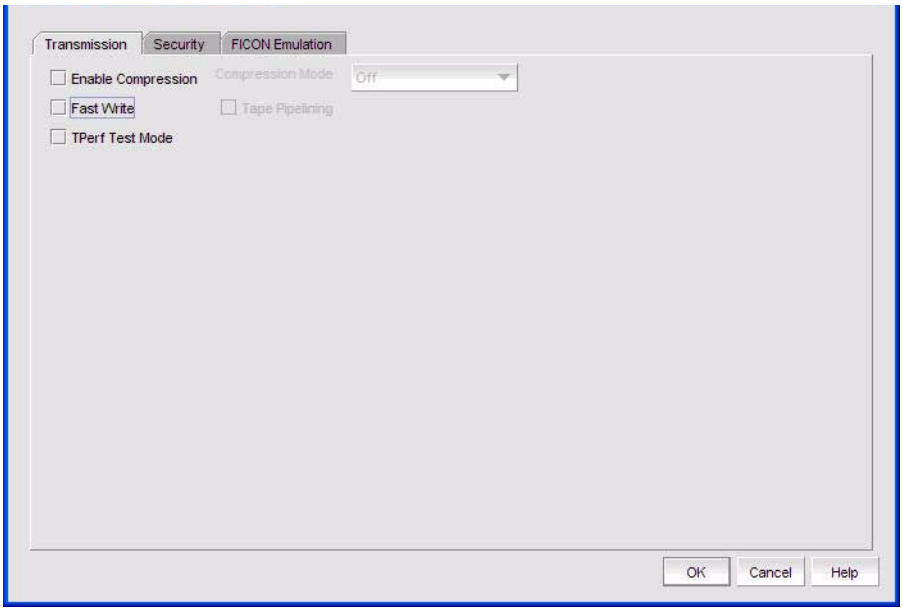


FIGURE 72 Advanced Settings Transmission tab

Enabling and disabling compression

The procedure for enabling compression for the 4 Gbps Router, Extension Switch and Blade is different than the procedure for enabling compression for the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade.

For 4 Gbps Router, Extension Switch and Blade:

1. Select the **Enable Compression** check box to enable compression.
2. Click **OK** to commit your selection.

For the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade:

1. Select the **Enable Compression** check box to enable compression.

   This enables the **Compression Mode** selector.
2. Values of 1, 2, and 3 are available from the **Compression Mode** selector. A value of 1 enables the normal hardware compression mode for the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and the 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade. Values of 2 and 3 set incrementally more aggressive software compression modes. A value of 2 sets moderate compression mode, and a value of 3 sets aggressive compression mode.
3. Click **OK** to commit you selection.

To disable compression, click the **Enable Compression** to clear the check mark, and click **OK.**

Enabling Open Systems Tape Pipelining (OSTP)

To enable OSTP, do the following:

1. Select the **Fast Write** check box.

   This enables the Tape Pipelining check box.
2. Select the **Tape Acceleration** check box.
3. Click **OK**.

Enabling Tperf test mode

Tperf test mode should not be enabled during normal operations. It is only used for testing and troubleshooting tunnels. Refer to the *Fabric OS FCIP Administrator's Guide* for information about Tperf.

Configuring IPSec and IKE policies

IPSec and IKE policies are configured from the **Security** tab (Figure 73). IPSec and IKE policy creation is an independent procedure. These policies must be known to you before you can configure them.

NOTE
Fabric OS version 6.3.0 does not support IPSec on the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade.

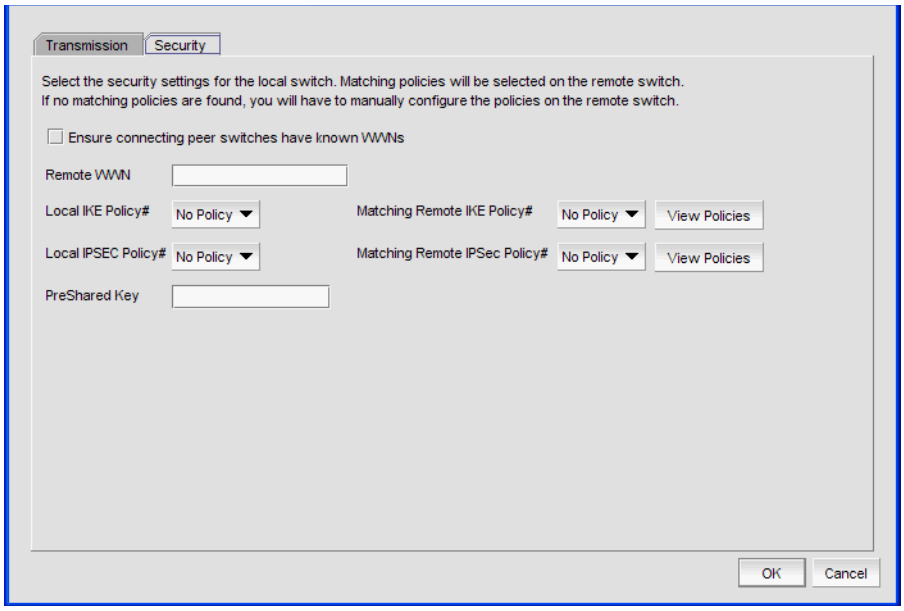

Transmission
Security
Select the security settings for the local switch. Matching policies will be selected on the remote switch.
If no matching policies are found, you will have to manually configure the policies on the remote switch.
Ensure connecting peer switches have known WWNs
Remote WWN
Local IKE Policy#
No Policy
Matching Remote IKE Policy#
No Policy
View Policies
Local IPSEC Policy#
No Policy
Matching Remote IPSec Policy#
No Policy
View Policies
PreShared Key
OK
Cancel

FIGURE 73 **Advanced Settings Security tab**

These policies are used to make the connection more secure through authentication and encryption. When you select a policy for the local switch, a matching policy is automatically selected on the remote switch. If no matching policy is found, you must manually configure the policy on the remote switch.

If the IPSec policy is selected, you must specify the preshared key. The **Preshared Key** is the key to be used during IKE/IPSec authentication. It must be between 12 and 32 alphanumeric characters. It must also be an exact match on both switches.

NOTE
IPSec settings cannot be edited. If you want to change settings, you will need to delete the tunnel and then create a new tunnel with the new settings.

Configuring FICON emulation

FICON emulation and acceleration features and operating parameters are configured from the **FICON Emulation** tab (Figure 74). Before you configure these features you must decide which features you want to implement, and you must look closely at the operational parameters to determine if values other than the default values are better for your installation.

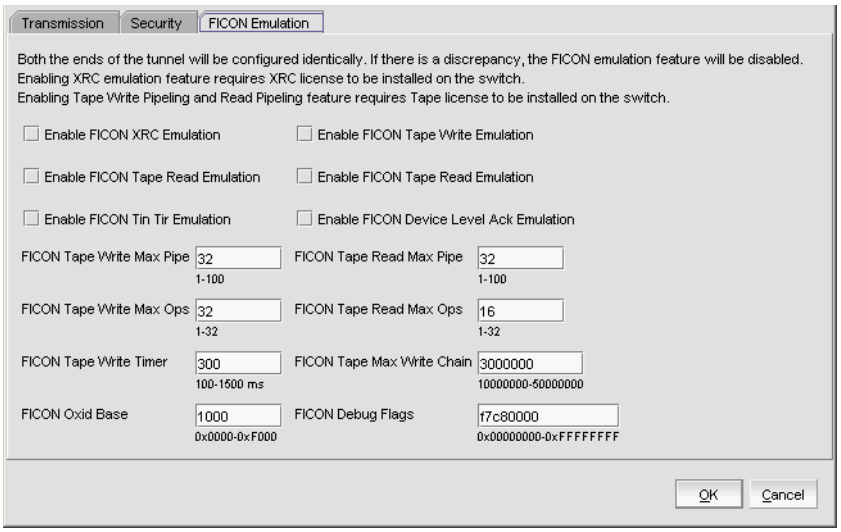


FIGURE 74 FICON Emulation configuration tab

1. Select the check boxes for the FICON emulation features you want to implement.

NOTE
The primary FICON emulation features are XRC emulation, tape write pipelining, and tape read pipelining. TIN/TUR emulation and device level ACK emulation provide support for the three primary features. If you select any of the primary features, you must also select TIN/TUR emulation and device level ACK emulation.

2. Select the operational parameters for FICON emulation.
   - **FICON Tape Write Max Pipe** defines a maximum number of channel commands that may be outstanding at a given time during write pipelining. Too small of a value will result in poor performance. The value should be chosen carefully based upon the typical tape channel program that requires optimum performance. The range is 1-100.
   - **FICON Tape Read Max Pipe** defines a maximum number of channel commands that may be outstanding at a given time during read pipelining. Too small of a value will result in poor performance. The value should be chosen carefully based upon the typical tape channel program that requires optimum performance. The range is 1-100.
   - **FICON Tape Write Max Ops** defines a maximum number of concurrent emulated tape write operations. The range is 1-32.

- **FICON Tape Read Max Ops** defines a maximum number of concurrent emulated tape read operations. The range is 1-32.
- **FICON Tape Write Timer** defines a time limit for pipelined write chains. This value is be specified in milliseconds (ms). If a pipelined write chain takes longer than this value to complete, the ending status for the next write chain will be withheld from the channel. This limits processing to what the network and device can support. Too small a value limits pipelining performance. Too large a value results in too much data being accepted for one device on a path. The range is 100-1500.
- **FICON Tape Max Write Chain** defines the maximum amount of data that can be contained in a single CCW chain. If this value is exceeded, emulation is suspended.
- **FICON Oxid Base** defines the base value of an entry pool of 256 OXIDs supplied to emulation generated exchanges. It should fall outside the range used by FICON channels and devices to avoid conflicts. The range is 0x0000 to 0xF000.
- **FICON Debug Flags** defines optional debug flags. This is primarily for use by technical support personnel.

Viewing FCIP connection properties

The FCIP connection properties show properties of the blades or switches on both sides of a connection. To view FCIP connection properties, right-click the connection between two extension blades or switches (Figure 75).

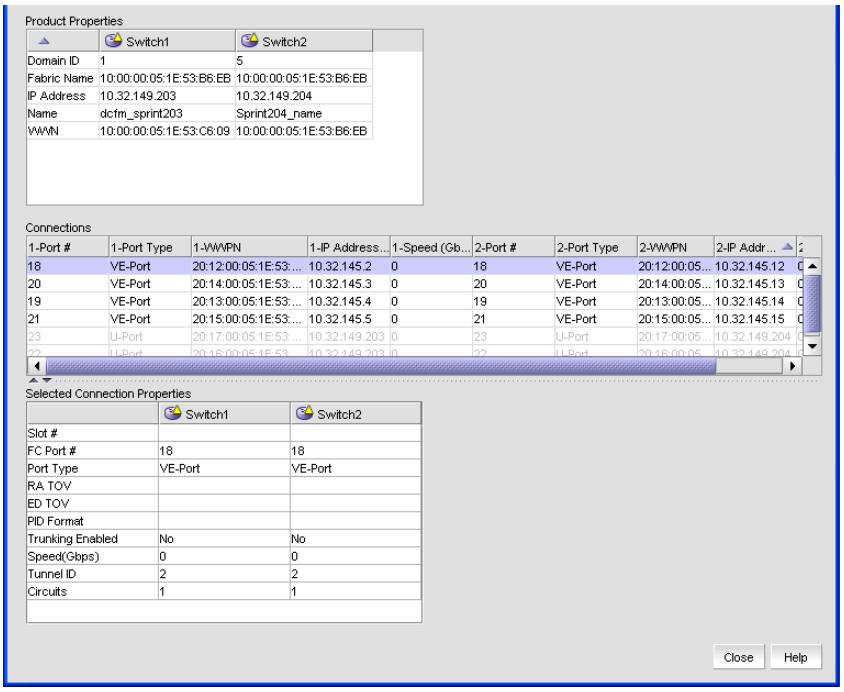

Product Properties
Switch1
Switch2
Domain ID 1 5
Fabric Name 10:00:00:05:1E:53:B6:EB 10:00:00:05:1E:53:B6:EB
IP Address 10.32.149.203 10.32.149.204
Name dcfm_sprint203 Sprint204_name
WWN 10:00:00:05:1E:53:C6:09 10:00:00:05:1E:53:B6:EB
Connections
1-Port # 1-Port Type 1-WWPN 1-IP Address... 1-Speed (Gb... 2-Port # 2-Port Type 2-WWPN 2-IP Addr...
18 VE-Port 20:12:00:05:1E:53:... 10.32.145.2 0 18 VE-Port 20:12:00:05... 10.32.145.12
20 VE-Port 20:14:00:05:1E:53:... 10.32.145.3 0 20 VE-Port 20:14:00:05... 10.32.145.13
19 VE-Port 20:13:00:05:1E:53:... 10.32.145.4 0 19 VE-Port 20:13:00:05... 10.32.145.14
21 VE-Port 20:15:00:05:1E:53:... 10.32.145.5 0 21 VE-Port 20:15:00:05... 10.32.145.15
23 U-Port 20:17:00:05:1E:53:... 10.32.149.203 0 23 U-Port 20:17:00:05... 10.32.149.204
Selected Connection Properties
Switch1
Switch2
Slot #
FC Port # 18 18
Port Type VE-Port VE-Port
RA TOV
ED TOV
PID Format
Trunking Enabled No No
Speed(Gbps) 0 0
Tunnel ID 2 2
Circuits 1 1
Close
Help

FIGURE 75 FCIP connection properties

Viewing General FCIP properties

Take the following steps to view general FCIP properties.

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **Properties** tab (Figure 76).

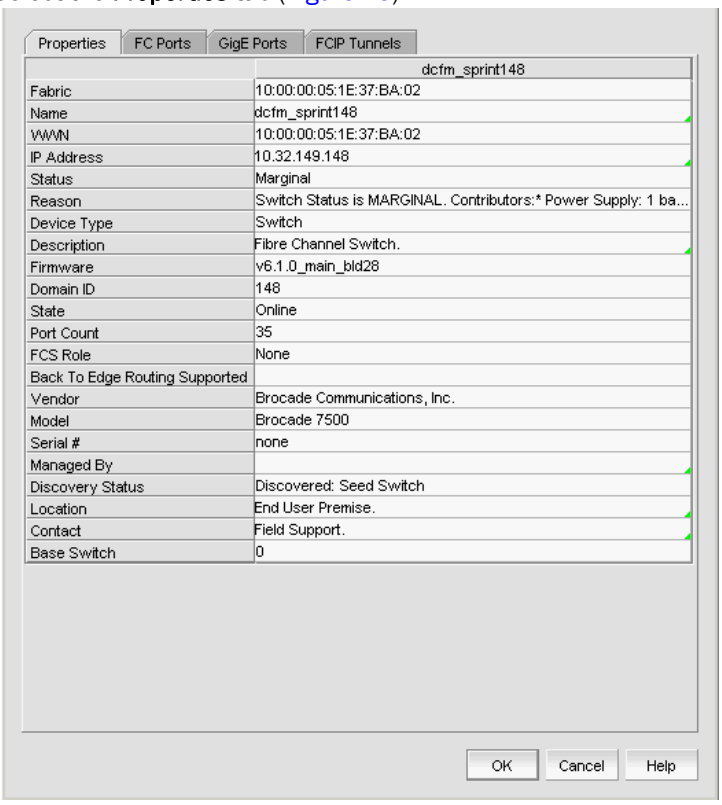


FIGURE 76 **General FCIP properties tab**

Viewing FCIP FC port properties

Take the following steps to view FCIP FC port properties.

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **FC Ports** tab (Figure 77).

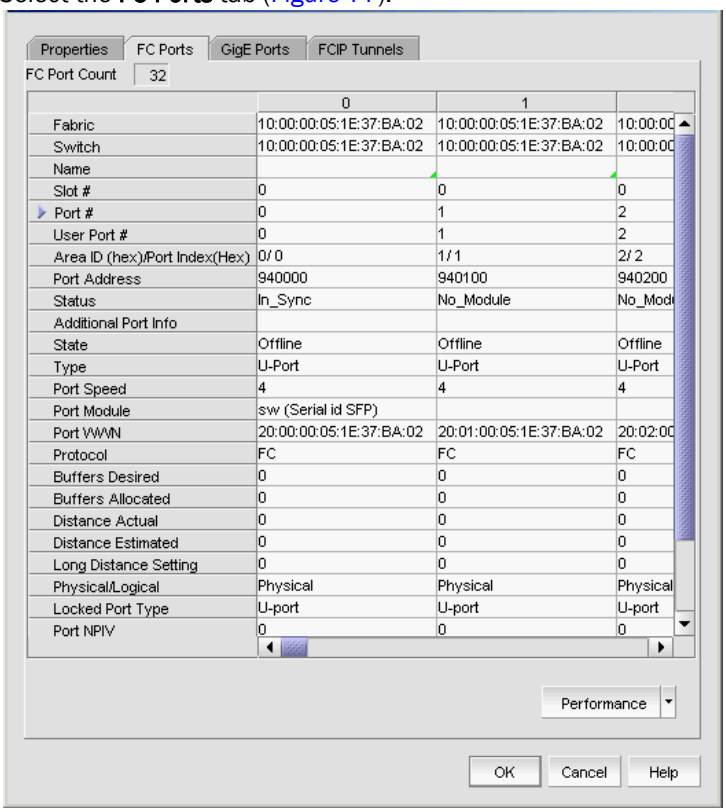


FIGURE 77 **FC ports tab**

Viewing FCIP Ethernet port properties

Take the following steps to view Ethernet port properties.

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **GigE Ports** tab (Figure 78).

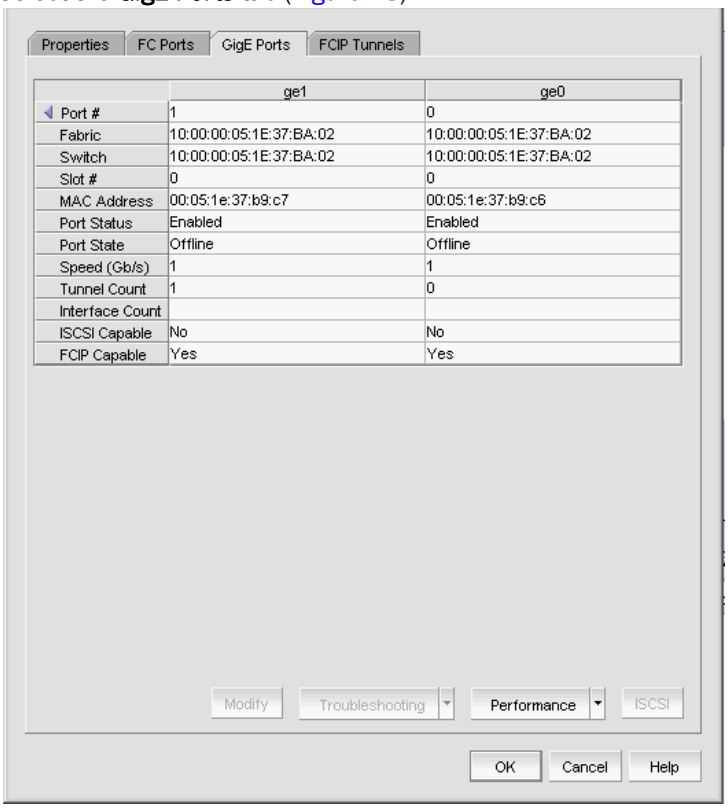


FIGURE 78 GigE ports tab

Editing FCIP tunnels

NOTE
You cannot edit an active tunnel; disable the tunnel before making changes.

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to edit.
2. Select **Edit Tunnel**.

   The **Edit FCIP Tunnel** dialog box displays (Figure 79).

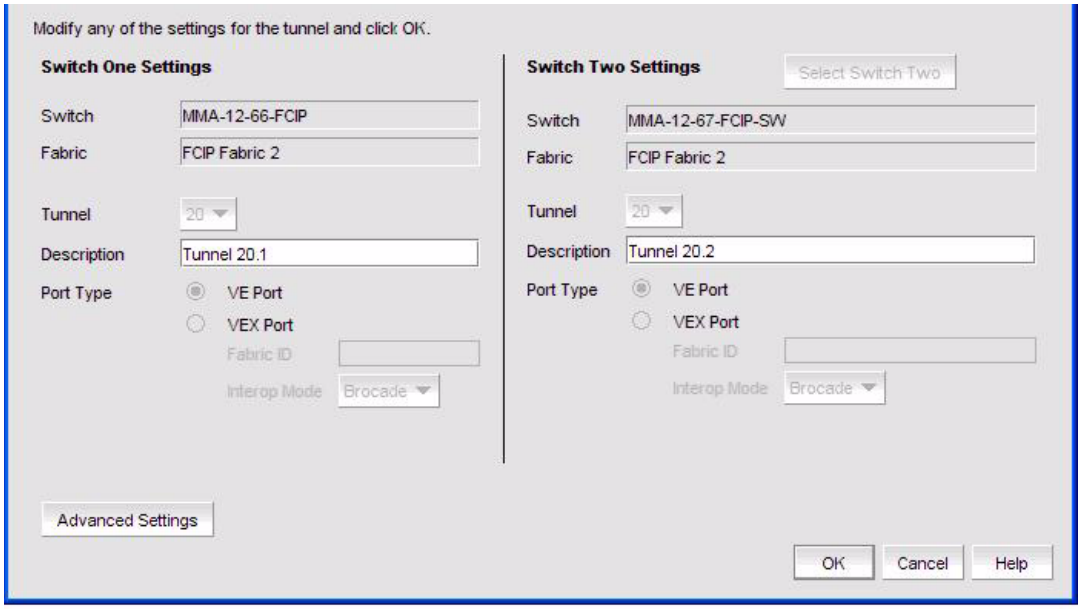


FIGURE 79 **Edit FCIP Tunnel dialog box**

3. Fields and parameters are as described in Configuring an FCIP tunnel. You can edit all editable fields and parameters.

Editing FCIP circuits

FCIP circuit settings may be edited from the **Edit FCIP Circuit** dialog box. The procedure for launching this dialog box for the 4 Gbps Router, Extension Switch and Blade is different than the procedure for the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and the 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade. The 4 Gbps Router, Extension Switch and Blade have only one circuit per tunnel, and the circuit is edited as part of the tunnel. The 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade may have multiple circuits per tunnel, and circuits may be selected individually.

For the 4 Gbps Router, Extension Switch and Blade:

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to edit.
2. Select **Edit Tunnel**.

   The **Edit FCIP Tunnel** dialog box displays.
3. Select **Edit FCIP Circuit**.

   The **Edit FCIP Circuit** dialog box displays.

For the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and the 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade:

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to edit.
2. Select the **Circuit** tab.
3. Select a circuit from the circuit properties table.
4. Select **Edit Circuit**.

   The **Edit FCIP Circuit** dialog box displays (Figure 80).

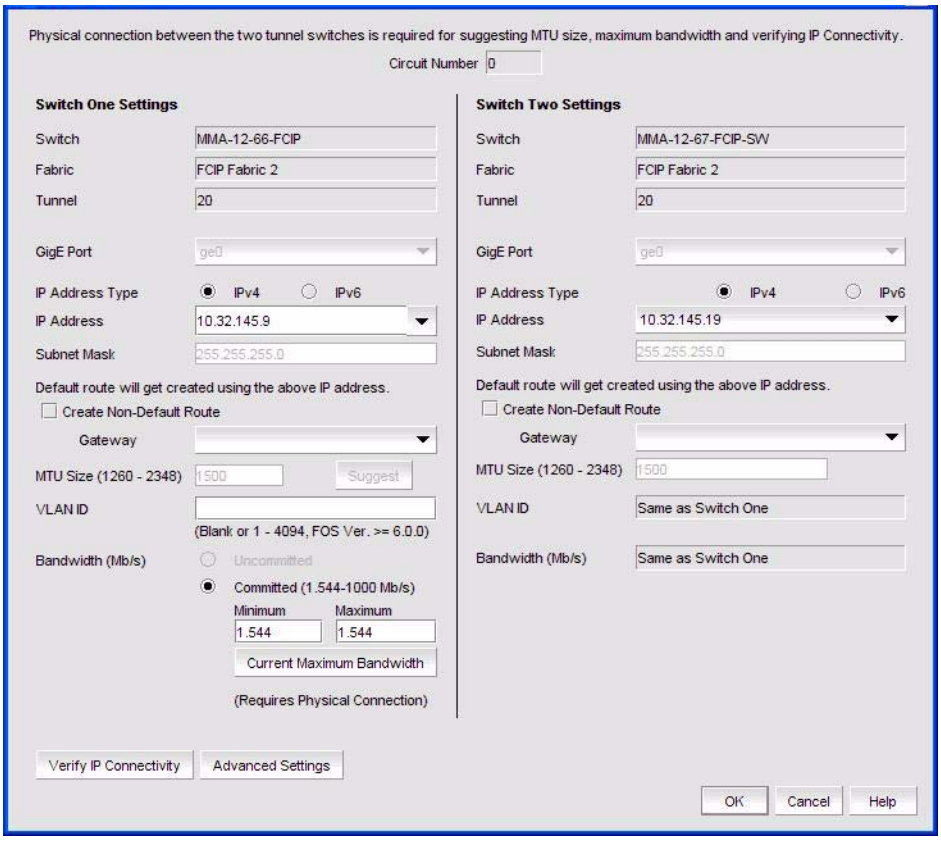


FIGURE 80 **Edit FCIP Circuits dialog box**

5. Fields and parameters are as described in Adding an FCIP circuit. You can edit all editable fields and parameters.

Disabling FCIP tunnels

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to disable.
2. Select **Disable Tunnel**.

   A confirmation dialog box displays, warning you that when you delete a tunnel, you delete all associated FCIP circuits.
3. Click **OK** to disable the tunnel.

Enabling FCIP tunnels

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to enable.
2. Select **Enable Tunnel**.

   A confirmation dialog box displays.
3. Click **OK** to enable the tunnel.

Deleting FCIP tunnels

1. From the **FCIP Tunnels** dialog box, right-click the tunnel you want to delete.
2. Select **Delete Tunnel**.

   A confirmation dialog box displays, warning you of the consequences of deleting a tunnel.
3. Click **OK** to delete the tunnel.

Disabling FCIP circuits

1. From the **FCIP Tunnels** dialog box, right-click the tunnel that contains the circuit.
2. Select the **Circuit** tab.
3. Select the circuit from the circuit properties table.
4. Select **Disable Circuit**.

   A confirmation dialog box displays.
5. Click **OK** to disable the circuit.

Enabling FCIP circuits

1. From the **FCIP Tunnels** dialog box, right-click the tunnel that contains the circuit.
2. Select the **Circuit** tab.
3. Select the circuit from the circuit properties table.
4. Select **Enable Circuit**.

   A confirmation dialog box displays.
5. Click **OK** to enable the circuit.

Deleting FCIP Circuits

1. From the **FCIP Tunnels** dialog box, right-click the tunnel that contains the circuit.
2. Select the **Circuit** tab.
3. Select the circuit from the circuit properties table.
4. Select **Delete Circuit**.

   A confirmation dialog box displays, warning you of the consequences of deleting a circuit.
5. Click **OK** to delete the circuit.

Displaying FCIP performance graphs for FC ports

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **FC Ports** tab.
3. Click **Performance > Real Time Graph**.

Displaying FCIP performance graphs for Ethernet ports

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **GigE Ports** tab.
3. Click **Performance > Real Time Graph**.

Displaying link details for FCIP tunnels

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension switch or chassis that contains an extension blade on the Connectivity Map, and select **Properties**.
2. Select the **FCIP Tunnels** tab.
3. Click **Properties**.

   The **Connection Properties** dialog box for the selected tunnel is displayed.

Displaying tunnel properties from the FCIP tunnels dialog box

Tunnel properties can be displayed from the **FCIP Tunnels** dialog box.

1. Select a tunnel from the **FCIP tunnels** dialog box.
2. Select the **Tunnel** tab.

   Tunnel properties are displayed (Figure 81).

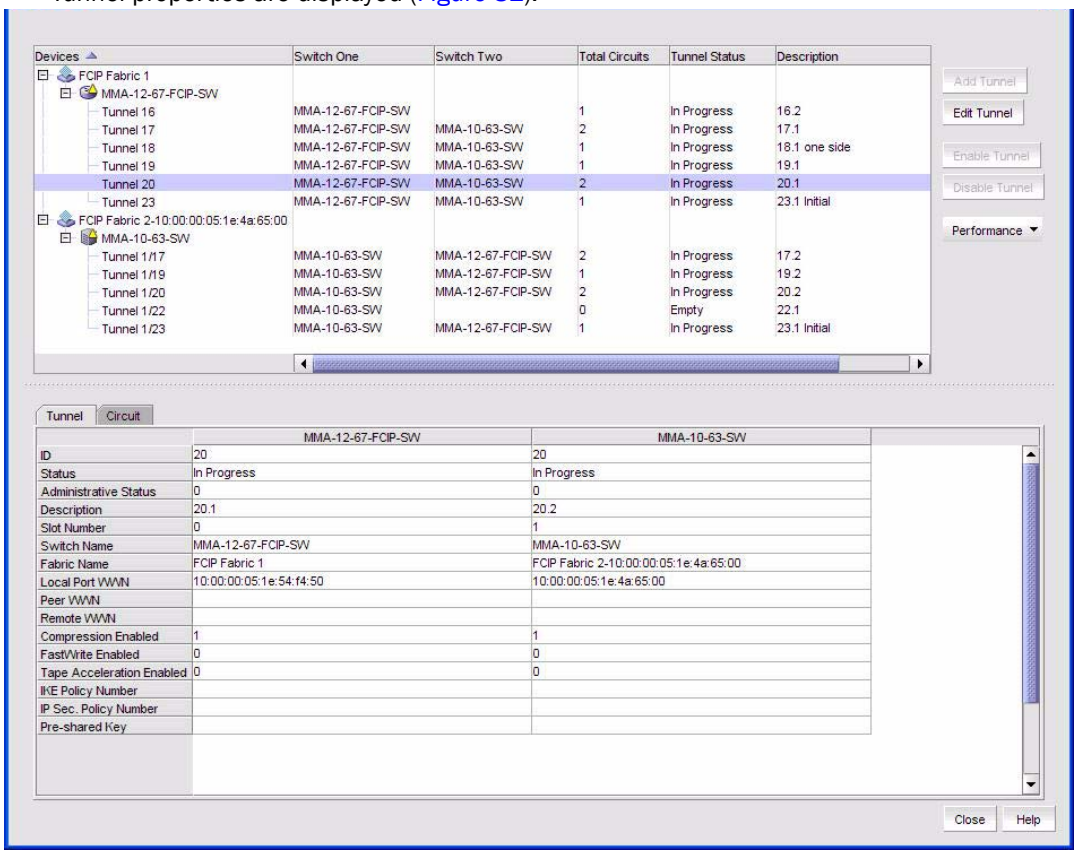


FIGURE 81 **Tunnel properties on the FCIP Tunnels dialog box**

Displaying FCIP circuit properties from the FCIP tunnels dialog box

Tunnel properties can be displayed from the **FCIP Tunnels** dialog box using the following procedure.

1. Select a tunnel from the **FCIP tunnels** dialog box.
2. Select the **Circuit** tab.

   Circuit properties are displayed (Figure 82).

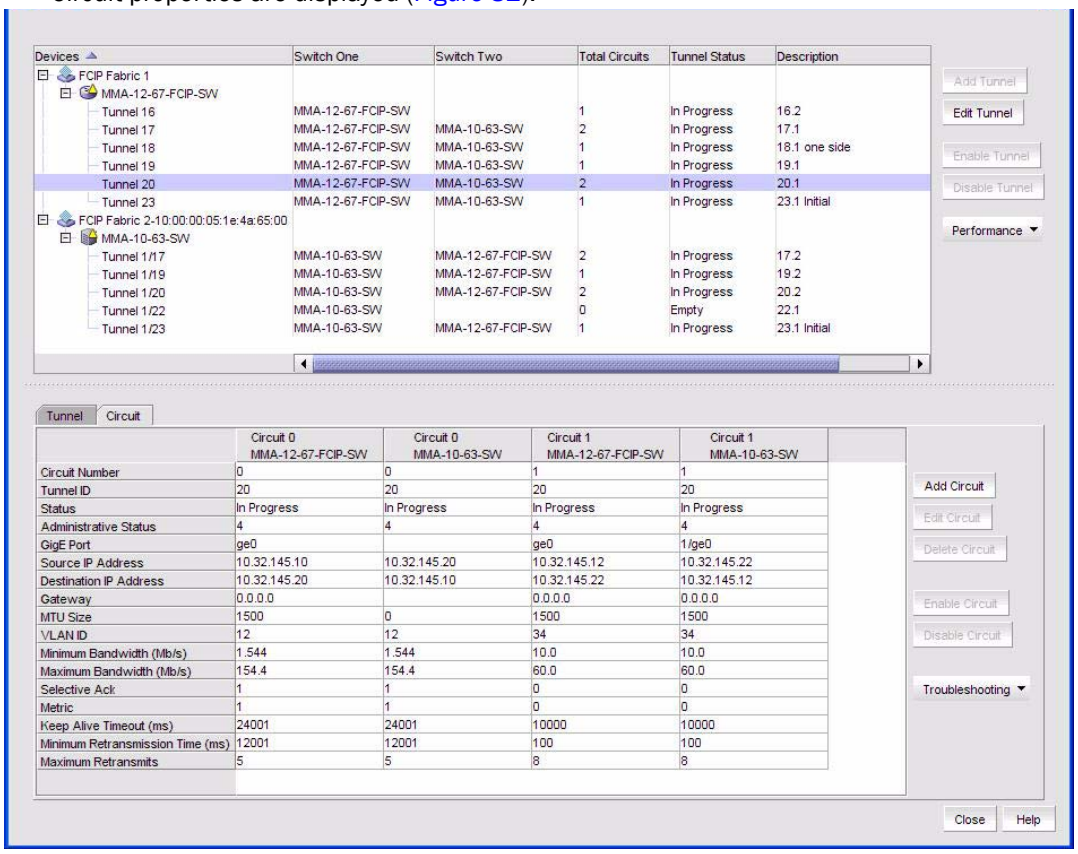

Devices
Switch One
Switch Two
Total Circuits
Tunnel Status
Description
FCIP Fabric 1
MMA-12-67-FCIP-SW
Tunnel 16 MMA-12-67-FCIP-SW 1 In Progress 16.2
Tunnel 17 MMA-12-67-FCIP-SW MMA-10-63-SW 2 In Progress 17.1
Tunnel 18 MMA-12-67-FCIP-SW MMA-10-63-SW 1 In Progress 18.1 one side
Tunnel 19 MMA-12-67-FCIP-SW MMA-10-63-SW 1 In Progress 19.1
Tunnel 20 MMA-12-67-FCIP-SW MMA-10-63-SW 2 In Progress 20.1
Tunnel 23 MMA-12-67-FCIP-SW MMA-10-63-SW 1 In Progress 23.1 Initial
FCIP Fabric 2-10:00:00:05:1e:4a:65:00
MMA-10-63-SW
Tunnel 1/17 MMA-10-63-SW MMA-12-67-FCIP-SW 2 In Progress 17.2
Tunnel 1/19 MMA-10-63-SW MMA-12-67-FCIP-SW 1 In Progress 19.2
Tunnel 1/20 MMA-10-63-SW MMA-12-67-FCIP-SW 2 In Progress 20.2
Tunnel 1/22 MMA-10-63-SW 0 Empty 22.1
Tunnel 1/23 MMA-10-63-SW MMA-12-67-FCIP-SW 1 In Progress 23.1 Initial
Add Tunnel
Edit Tunnel
Enable Tunnel
Disable Tunnel
Performance
Tunnel
Circuit
Circuit 0 MMA-12-67-FCIP-SW
Circuit 0 MMA-10-63-SW
Circuit 1 MMA-12-67-FCIP-SW
Circuit 1 MMA-10-63-SW
Circuit Number 0 0 1 1
Tunnel ID 20 20 20 20
Status In Progress In Progress In Progress In Progress
Administrative Status 4 4 4 4
GigE Port ge0 ge0 1/ge0
Source IP Address 10.32.145.10 10.32.145.20 10.32.145.12 10.32.145.22
Destination IP Address 10.32.145.20 10.32.145.10 10.32.145.22 10.32.145.12
Gateway 0.0.0.0 0.0.0.0 0.0.0.0
MTU Size 1500 0 1500 1500
VLAN ID 12 12 34 34
Minimum Bandwidth (Mb/s) 1.544 1.544 10.0 10.0
Maximum Bandwidth (Mb/s) 154.4 154.4 60.0 60.0
Selective Ack 1 1 0 0
Metric 1 1 0 0
Keep Alive Timeout (ms) 24001 24001 10000 10000
Minimum Retransmission Time (ms) 12001 12001 100 100
Maximum Retransmits 5 5 8 8
Add Circuit
Edit Circuit
Delete Circuit
Enable Circuit
Disable Circuit
Troubleshooting
Close
Help

FIGURE 82 **Circuit properties on the FCIP Tunnels dialog box**

Displaying switch properties from the FCIP Tunnels dialog box

Switch properties are displayed on the **FCIP Tunnels** dialog box when you select a switch (Figure 83).

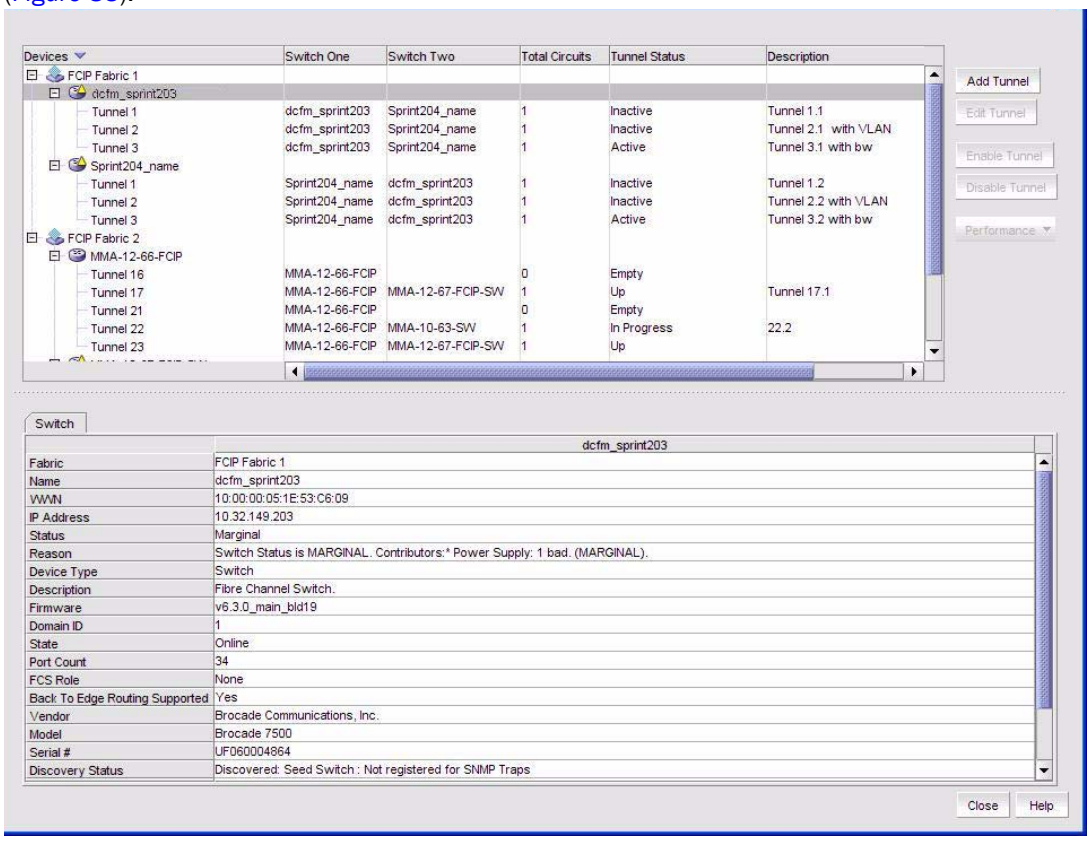


FIGURE 83 **Switch properties on the FCIP Tunnels dialog box**

Displaying fabric properties from the FCIP Tunnels dialog box

Fabric properties are displayed on the FCIP Tunnels dialog box when you select a switch. (Figure 84).

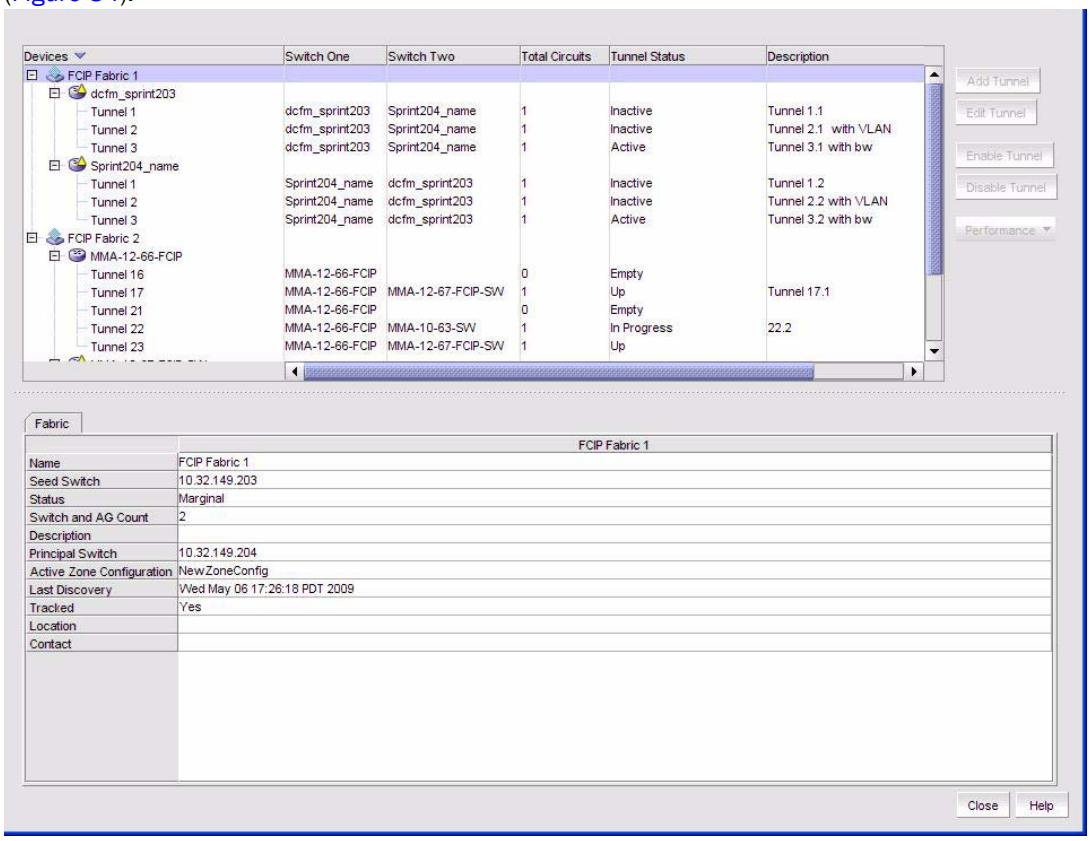


FIGURE 84 **Fabric properties on the FCIP Tunnels dialog box**

Troubleshooting FCIP Ethernet connections

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **GigE Ports** tab.
3. Select the Ethernet port.
4. Click **Troubleshooting**.

   The following options are presented:

   - **ipPerf**—Measures end-to-end IP path performance between a pair of FCIP ports (4 Gbps Router, Extension Switch and Blade only).
   - **ip ping**—Tests connections between a local Ethernet port (ge0 or ge1) and a destination IP address.
   - **ip traceroute**—Traces routes from a local Ethernet port (ge0 or ge1) to a destination IP address.

Chapter

11

Fibre Channel over Ethernet

In this chapter

- FCoE overview 267
- QoS configuration 282
- LLDP-DCBX configuration 291
- Access Control List configuration 296
- Spanning Tree Protocol configuration 302
- 802.1x authentication. 307
- Virtual FCoE port configuration 310

FCoE overview

Fibre Channel over Ethernet (FCoE) leverages Ethernet enhancements, called *Converged Enhanced Ethernet (CEE),* to transport encapsulated Fibre Channel frames over Ethernet. Ethernet is the physical layer over which the encapsulated FC frames are transported.

One of the barriers to using Ethernet as the basis for a converged network has been the limited bandwidth that Ethernet has historically provided. However, with 10 Gbps Ethernet, the available bandwidth now offers the potential to consolidate all the traffic types over the same link.

Unlike Fibre Channel, Ethernet is not a peer-to-peer protocol. The mechanism used to discover new ports, MAC address assignments and FC logins and logouts is called the FCoE Initialization Protocol (FIP).

DCB exchange protocol

DCB Exchange (DCBX) protocol allows enhanced Ethernet devices to convey and configure their CEE capabilities and ensures a consistent configuration across the network. DCBX protocol is used between data center bridging (DCB) devices, such as a converged network adapter (CNA) and a FCoE switch, to exchange configuration with directly-connected peers.

NOTE
When DCBX protocol is used, any other LLDP implementation must be disabled on the host systems.

Enhanced Ethernet features

Converged Enhanced Ethernet (CEE) is a set of IEEE 802 standard Ethernet enhancements that enable Fibre Channel convergence with Ethernet. The two basic requirements in a lossless Ethernet environment are Enhanced Transmission Selection (ETS) and priority-based flow control. These capabilities allow the Fibre Channel frames to run directly over 10 Gbps Ethernet segments without adversely affecting performance.

Enhanced transmission selection

Enhanced transmission selection (ETS) allows lower priority traffic classes to use available bandwidth that is not be used by higher priority traffic classes and maximizes the use of available bandwidth.

ETS allows configuration of bandwidth per priority group.

Priority group ID usage is defined as follows:

- PGID = {0, 7} is used when the priority group is limited for its bandwidth use.
- PGID = {8, 14} is reserved.
- PGID = {15} is used for priorities that are not limited for their bandwidth use.

The configured priority group percentage refers to the maximum percentage of available link bandwidth after PGID 15 is serviced, assuming all priority groups are fully subscribed. If one of the priority groups does not consume its allocated bandwidth, then any unused portion is available for use by other priority groups.

Priority-based flow control

Priority-based flow control allows the network to selectively pause different classes of traffic and create lossless lanes for Fibre Channel, while retaining packet drop congestion management for IP traffic. A high-level pause example follows:

- During periods of heavy congestion, the receive buffers reach high threshold and generate a pause.
- The pause tells transmission (Tx) queues to stop transmitting.
- After the receive (Rx) buffers reach low threshold, a zero pause is generated.
- The zero pause signals the Tx queues to resume transmitting.

Ethernet jumbo frames

The basic assumption underlying FCoE is that TCP/IP is not required in a local data center network and the necessary functions can be provided with Enhanced Ethernet. The purpose of an “enhanced” Ethernet is to provide reliable, lossless transport for the encapsulated Fibre Channel traffic. Enhanced Ethernet provides support for jumbo Ethernet frames and in-order frame delivery.

The Brocade FCoE 10 Gbps converged network adapter supports jumbo packets of up to 9 KB, compared to the original 1,518-byte MTU for Ethernet. The frame size increase allows the same amount of data to be transferred with less effort.

FCoE protocols supported

The Brocade FCoE converged network adapter supports two layers of protocols: Ethernet link layer and FCoE layer. They are listed in the following sections.

Ethernet link layer protocols supported

The following protocols support the Ethernet link layer.

- 802.1q (VLAN)
- 802.1Qaz (enhanced transmission selection)
- 802.1Qbb (priority flow control)
- 802.3ad (link aggregation)
- 802.3ae (10 Gb Ethernet)
- 802.1p (priority encoding)
- IEEE 1149.1 (JTAG) for manufacturing debug and diagnostics
- IPv4 specification (RFC 793/768)
- IPv6 specification (RFC 2460)
- TCP/UDP specification (RFC 793/768)
- ARP specification (RFC 826)
- RSS with support for IPV4TCP, IPV4, IPV6TCP, IPV6 hash types
- HDS (Header-data split)

FCoE protocols

The following protocols support Fibre Channel over Ethernet.

- FIP (FC-BB5 compliant):
  - Support for FIP Discovery protocol for dynamic FCF discovery and FCoE link management
  - Support for FPMA and SPMA type FIP fabric login
- Support for Initiator mode only (FCP-3 compliant in Initiator mode)
- SCSI protection information support
- IP-over-FC
- NPIV support

CEE configuration

This switch has eight 8 Gbps FC ports and 24 10 Gbps Ethernet CEE ports. You must configure CEE interfaces and ports differently than you configure FC ports, in order to effectively use the converged network features.

For example, Priority-based flow control (PFC) and Enhanced transmission selection (ETS) are the two QoS policy enhancements you must configure to create a lossless Ethernet. You then use DCBX protocol on CEE-enabled devices to exchange configuration information.

Switch, CEE port, and link aggregation group (LAG) policies are discussed later in this chapter.

Opening the CEE Configuration dialog box

To access the CEE Configuration dialog box, complete the following steps.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

NOTE
You can also launch the **CEE Configuration** dialog box from the 8 Gbps 16-FC-ports, 10 GbE 8-Ethernet Port switch by right-clicking the switch in the product device tree or topology map and selecting **Configuration > CEE**.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

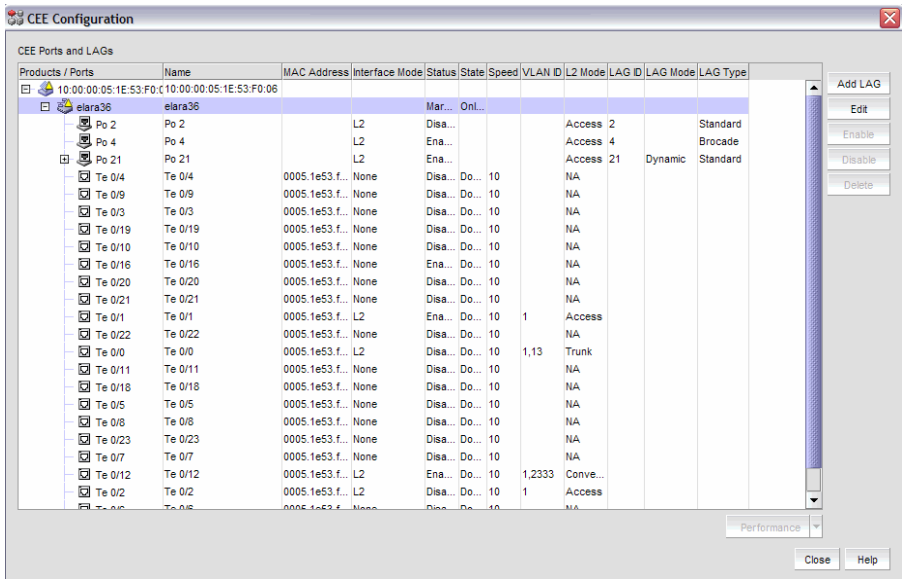


FIGURE 85 CEE switch configuration dialog box

2. Select the CEE switch, link aggregation group, or CEE port to perform the converged enhanced Ethernet task.

CEE configuration tasks

The **CEE Configuration** dialog box enables you to perform the following tasks:

- Edit CEE ports for a selected switch. You can also add a link aggregation group (LAG) if a single switch is selected.
- Edit a switch or port and configure the following CEE policies:

  NOTE
  Access Control List and Spanning Tree Protocol can also be set at the LAG level.

  - QoS
  - LLDP-DCBX
  - Access Control List
  - Spanning Tree Protocol
  - 802.1x
- Enable or disable a LAG or CEE port.
- Display performance statistics for CEE ports.

Instructions for performing the CEE configuration tasks are detailed in the following sections:

- "Link aggregation groups" on page 273
- "QoS configuration" on page 282
- "LLDP-DCBX configuration" on page 291
- "Access Control List configuration" on page 296
- "Spanning Tree Protocol configuration" on page 302
- "802.1x authentication" on page 307

Switch policies

You can configure and enable a number of CEE policies on a switch, port, or link aggregation group (LAG).

The following switch policy configurations apply to all ports in a LAG:

- CEE map and Traffic Class map
- Link Layer Discovery Protocol (LLDP)

The following switch policy configurations apply to the LAG itself:

- Access Control Lists (ACL)
- Spanning Tree Protocol (STP)

The switch policies are described in the following sections.

CEE map and Traffic Class map

With CEE, Fibre Channel uses a buffer management system based on buffer-to-buffer credits, with corresponding confirmation by the R-RDY frame. The flow control standard used for CEE is based on “pause” frames. Coupled with an appropriate input buffer, lossless transport of frames is possible.

Priority-based flow control (PFC) deals with the prioritization of frames. This standard IEEE 802.1Q allows application-specific bandwidth reservations in CEE. When you create a CEE map, you specify the precedence (priority) and then you map the priority groups with the Class of Service (CoS) and apply bandwidth percentages.

Refer to “QoS configuration” on page 282 for instructions on how to create CEE and Traffic Class maps.

LLDP profiles

Data Center Bridging Capability Exchange Protocol (DCBX) enables Enhanced Ethernet devices to discover whether a peer device supports particular features, such as Priority Flow Control or Class of Service (CoS). In a Converged Enhanced Ethernet (CEE) environment, LLDP is enhanced with DCBX protocol to further share or change the configured CEE enhancements.

Refer to “LLDP-DCBX configuration” on page 291 for instructions on how to create LLDP profiles.

Access control lists

Access control lists (ACL) are sequential lists consisting of permit and deny rules. They are either Layer 3 (IP)- or Layer 2 (MAC)-specific. You can configure multiple access lists and rules and store them in the configuration. You create an ACL on a switch and then you can apply the configuration to ports, and link aggregation groups (LAGs) on that switch.

Refer to “Access Control List configuration” on page 296 for instructions on how to create and manage access control lists.

Spanning Tree Protocol policy

The Spanning Tree Protocol (STP) is a Layer 2 protocol that ensures a loop-free topology for any bridged LAN (Layer-2 bridges are typically Ethernet switches). Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops or the need to manually enable or disable these backup links.

Refer to "Spanning Tree Protocol configuration" on page 302 for more information.

802.1x policy

802.1x is a standard authentication protocol that defines a client-server-based access control and authentication protocol. 802.1x restricts unknown or unauthorized clients from connecting to a LAN through publicly accessible ports.

Refer to "802.1x authentication" on page 307 for information on setting 802.1x parameters.

Link aggregation groups

Link aggregation, based on the IEEE 802.3ad protocol, is a mechanism to bundle several physical ports together to form a single logical channel or trunk. The collection of ports is called a link aggregation group (LAG).

The **Add LAG** button is enabled when a single CEE switch or ports of a single CEE switch are selected. The **Add LAG** button is disabled when multiple switches are selected, ports from different switches are selected, or LAGs are selected.

The **Edit button** is enabled when a single LAG, port, or switch is selected.

NOTE
When LLDP-DCBX, Access Control List (ACL), or Spanning Tree Protocol (STP) is disabled on the switch, a yellow banner displays on the dialog box, indicating that LLDP-DCBX, ACL, or STP is not only disabled on the switch, it is also disabled for all ports and LAGs on the switch.

You manage port selection using the **Add LAG** dialog.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select the CEE switch or one or more CEE ports to add to a link aggregation group (LAG).

3. Click **Add LAG**.

   The **Add LAG** dialog box displays.

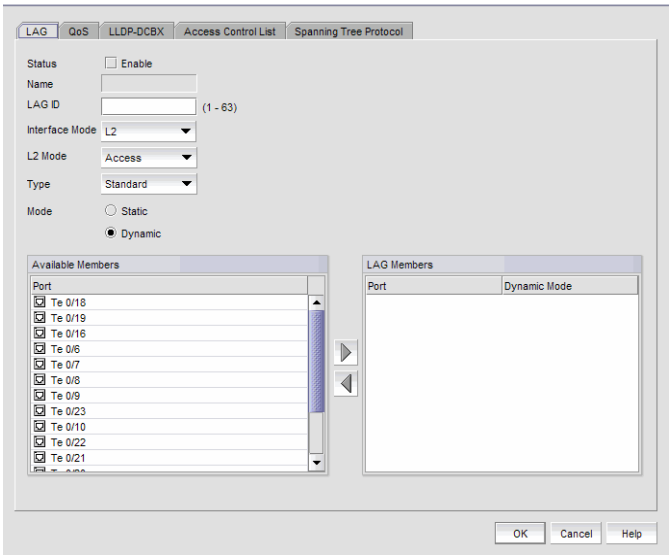


FIGURE 86 Add LAG dialog box

4. Configure the following LAG parameters:

NOTE
A LAG restriction exists whereby you can add 802.1x-enabled ports to a LAG, but the port will fail when the LAG is saved to the switch. 802.1x-enabled ports are not supported.

- **Status** - Enabled or Disabled. You must enable the LAG to use the CEE functionality.
- **Name** - The system-generated, read-only LAG name.
- **LAG ID** - Enter the LAG identifier, using a value between 1-63. Duplicate LAG IDs are not allowed.
- **Interface Mode** - L2 or None. Ports that are in L2 mode can't be added to a LAG.
- **L2 Mode** - Select the L2 mode (Access or Trunk).

5. Select at least one available CEE port from the **Available Members** table and click the right arrow button to move them to the **LAG Members** table.

   The CEE ports are now part of the link aggregation group.

6. Continue to configure the following LAG parameters. These parameters are disabled until you add a CEE port to the **LAG members** table.
   - **Mode -** Sets all ports added to the LAG members table in either Static or Dynamic mode. The default is Dynamic, Active, but LAG members can be Active or Passive if the LAG member is Dynamic.
   - **Type** - Sets the limit on the size of the LAG. The type values include Standard, where the LAG is limited to 16 ports, and Brocade, where the LAG is limited to four ports. The default is Standard.

     NOTE
     The 8 Gbps 16-FC-ports, 10 GbE 8-Ethernet Port has three anvil chips and each anvil chip supports eight 10 Gbps Ethernet ports. You cannot create Brocade-type LAGs from different anvil chips. If you do, an error message displays and only the first port is considered as part of the LAG.
7. When you have finished configuring the policies, click **OK**.

   The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

   If the operation was successful, the new LAG displays in the custom products list in the **CEE Configuration** dialog.

Editing a CEE switch

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select the CEE switch from the **Products/Ports** table.

3. Click **Edit**.

   The **Edit Switch** dialog box displays (Figure 87).

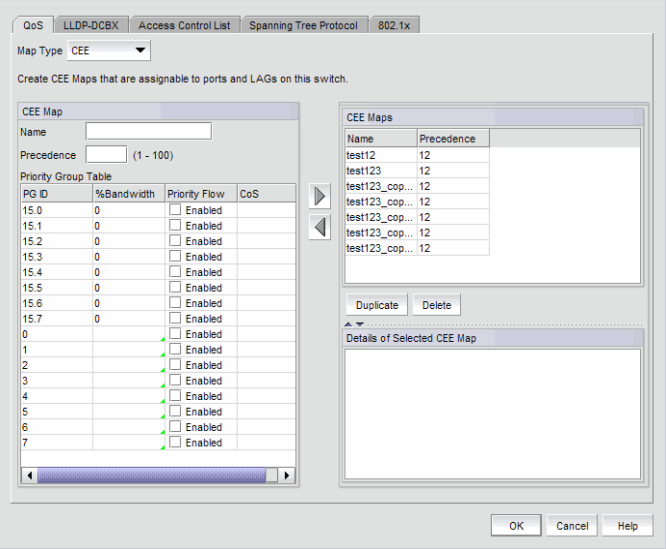


FIGURE 87 **Edit Switch dialog box**

4. Configure the policies for the Edit Switch tabs, which are described in the following sections:
   - "QoS configuration" on page 282
   - "LLDP-DCBX configuration" on page 291
   - "Access Control List configuration" on page 296
   - "Spanning Tree Protocol configuration" on page 302
   - "802.1x authentication" on page 307
5. When you have finished configuring the policies, apply the settings to the switch.
6. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.
7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Editing a CEE port

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a CEE port from the Products/Ports table.

3. Click **Edit**.

   The **Edit Port** dialog box displays.

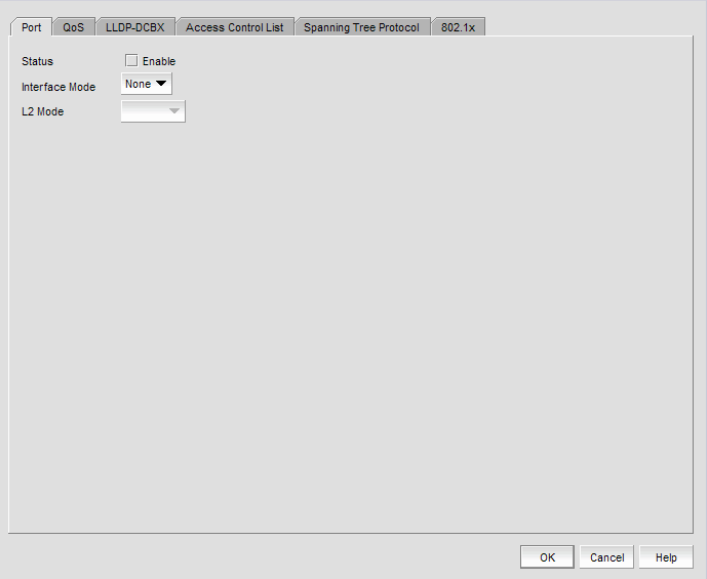


FIGURE 88 **Edit Port dialog box**

4. Modify the following CEE Port parameters as required:
   - **Status** - Enable or Disable. You must enable the LAG to use the CEE functionality.
   - **Interface Mode** - None or L2.
   - **L2 Mode** - This is enabled if you select L2 as the Interface Mode. You cannot change the Interface Mode to **None** if it is set to L2 and the port is assigned to a VLAN.
5. When you have finished configuring the policies, apply the settings to the CEE port.
6. Click **OK** when you have finished modifying the CEE port parameters.

   The **CEE Confirmation and Status** dialog box displays.
7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Editing a LAG

Use the following procedure to change members and policies in a link aggregation group (LAG).

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select the link aggregation group (LAG) from the Products/Ports table.

3. Click **Edit**.

   The **Edit LAG** dialog box displays.

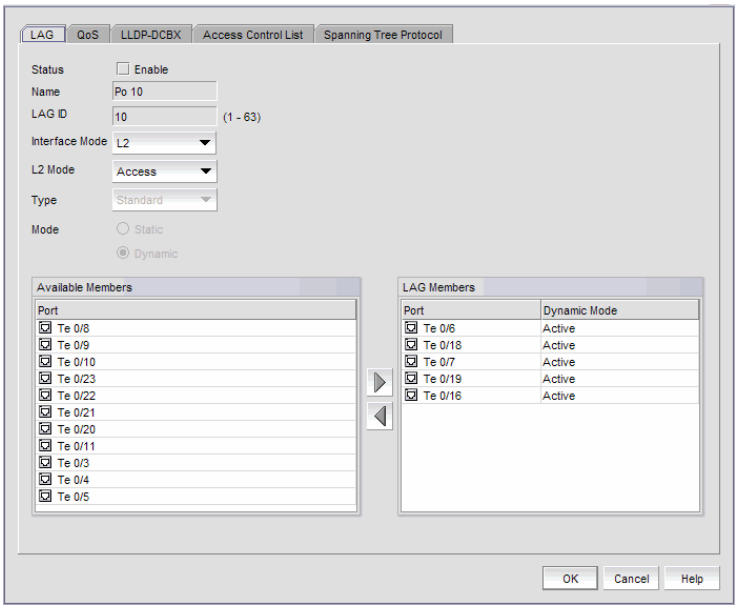


FIGURE 89 **Edit LAG dialog box**

4. Modify the following LAG parameters as required:
5. Configure the following LAG parameters:

NOTE
A LAG restriction exists whereby you can add 802.1x-enabled ports to a LAG, but the port will fail when the LAG is saved to the switch. 802.1x-enabled ports are not supported.

- **Status** - Enabled or Disabled. You must enable the LAG to use the CEE functionality.
- **Name** - The system-generated, read-only LAG name, assigned when the LAG is added.
- **LAG ID** - The LAG identifier, which is not an editable field.
- **Interface Mode** - L2 or none.
  - A port must be in L2 Mode if you are adding the port as a member of a LAG.
  - You cannot change the Interface Mode from **L2** to **none** if the LAG is assigned to a VLAN.
- **L2 Mode** - Select the L2 mode (Access or Trunk).

6. Select at least one available CEE port from the **Available Members** table and click the right arrow button to move them to the **LAG Members** table.

   The CEE ports are now part of the link aggregation group.

7. Continue to configure the following LAG parameters. These parameters are disabled until you add a CEE port to the **LAG members** table.
   - **Mode** - The ports that are LAG members are in either Static or Dynamic mode. You can change the mode of new port members only; you cannot change the mode on existing members of a LAG.

     If the mode is set as Dynamic, you can change the dynamic mode type (to Active or Passive) only for newly-added ports, not for existing port members of a LAG.
   - **Type** - The type value options are Standard, where the LAG is limited to 16 ports, and Brocade, where the LAG is limited to four ports. The default is **Standard**. The type is set when you add a LAG; you cannot edit the type using the **Edit LAG** dialog box.
8. Click **OK** when you have finished modifying the LAG parameters.

   The **CEE Confirmation and Status** dialog box displays.
9. Review the changes carefully before you accept them.
10. Click **Start** to apply the changes, or click **Close** to abort the operation.

Enabling a CEE port or LAG

If you select multiple switches or multiple ports and LAGs from two or more switches, both the **Enable** button and the **Disable** button are disabled.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select the CEE port or link aggregation group (LAG) that you want to enable.

   NOTE
   All selected LAGs must be in the same state (enabled or disabled); otherwise, both the **Enable** and **Disable** buttons are disabled.
3. Click **Enable**.

   The selected CEE port or LAG is enabled for CEE configuration.
4. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.
5. Review the changes carefully before you accept them.
6. Click **Start** to apply the changes, or click **Close** to abort the operation.

   The selected CEE port or LAG is enabled for CEE configuration. (The **Status** column in the **CEE Configuration** dialog reflects the change).

Disabling a CEE port or LAG

If you select multiple switches or multiple ports and LAGs from two or more switches, both the **Enable** button and the **Disable** button are disabled.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select one or more CEE ports or link aggregation groups (LAGs) that you want to disable.

   NOTE
   All selected LAGs must be in the same state (enabled or disabled); otherwise, both the **Enable** and **Disable** buttons are disabled.

3. Click **Disable**.
4. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

5. Review the changes carefully before you accept them.
6. Click **Start** to apply the changes, or click **Close** to abort the operation.

   The selected CEE port or LAG is disabled for CEE configuration. (The **Status** column in the **CEE Configuration** dialog reflects the state change).

Deleting a LAG

You can only delete a link aggregation group (LAG) that is selected from a single switch. If you select multiple switches or multiple LAGs from two or more switches, the **Delete** button is disabled.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select one or more LAGs that you want to delete from the **Products/Ports** table.
3. Click **Delete**.
4. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

5. Review the changes carefully before you accept them.
6. Click **Start** to apply the changes, or click **Close** to abort the operation.

   The LAG is removed from the **Products/Ports** list and any of the LAG members display without the LAG containment.

CEE Performance

Performance monitoring provides details about the quantity of traffic and errors a specific port or device generates on the fabric over a specific time frame. You can also use performance to indicate the devices that create the most traffic and to identify the ports that are most congested.

Real Time Performance Graph

You can monitor a device's performance through a performance graph that displays transmit and receive data. The graphs can be sorted by the column headers. You can create multiple real-time performance graph instances.

Generating a real-time performance graph.

To generate a real-time performance graph for a device, complete the following steps.

1. Select a CEE port from the **CEE Configuration** dialog box, and select **Real Time Graph** from the Performance list.

   A message displays, prompting you to close the **CEE Configuration** dialog box.

2. Click **OK** to close the **CEE Configuration** dialog and open the Performance dialog box.

   The **Real Time Performance Graphs** dialog box displays.

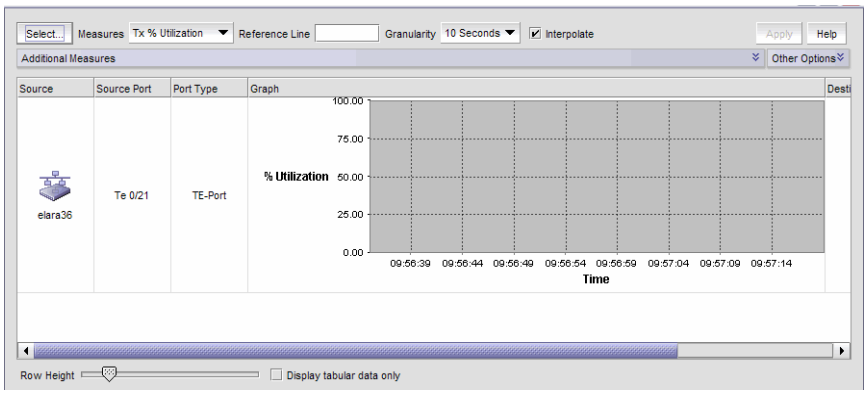


FIGURE 90 **Real Time Performance Graphs dialog box**

For complete information about Real Time Performance Graphs, refer to "Real-time performance data" on page 215.

Historical Performance Graph

The **Historical Performance Graph** dialog box enables you to customize how you want the historical performance information to display.

Generating a historical performance graph

1. Select a CEE port from the **CEE Configuration** dialog box, and select **Historical Graph** from the Performance list.

   A message displays, prompting you to close the **CEE Configuration** dialog.

2. Click **OK** to close the **CEE Configuration** dialog and open the Performance dialog box.

   The **Historical Performance Graph** dialog box displays.

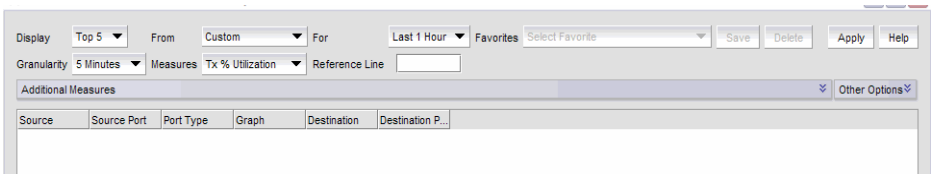


FIGURE 91 Historical Performance Graph dialog box

For complete information about Real Time Performance Graphs, refer to "Real-time performance data" on page 215.

QoS configuration

QoS configuration involves configuring packet classification, mapping the priority and traffic class, controlling congestion, and scheduling. The configuration of these QoS entities consist of CEE Map and Traffic Class Map configuration.

In a Converged Enhanced Ethernet (CEE) configuration, Enhanced Transmission Selection (ETS) and Priority-based flow control (PFC) are configured by utilizing a priority table, a priority group table, and a priority traffic table. The Traffic Class Map is the mapping of user priority to traffic class.

Enhanced Transmission Selection

Enhanced Transmission Selection (ETS) allows lower priority traffic classes to use available bandwidth not being used by higher priority traffic classes and maximizes the use of available bandwidth.

Priority-based flow control

Priority based flow control (PFC) is an enhancement to the existing pause mechanism in Ethernet. PFC creates eight separate virtual links on the physical link and allows any of these links to be paused and restarted independently, enabling the network to create a no-drop class of service for an individual virtual link.

Table 31 shows examples of how priority grouping might be allocated in a 15-priority group scenario.

TABLE 31 Priority table allocation example

Priority group ID	Bandwidth (%)	Priority flow control
0	55	on
1	25	on
2	0	off
3	0	off
4	5	off
5	0	off
6	15	on
7	0	off
15.0-15.7	Strict priority No bandwidth % configuration allowed	on

Creating a CEE map

When you create a CEE map, each of the Class of Service (CoS) options (0-7) must be mapped to at least one of the Priority Group IDs (0-7). All QoS, CEE map, and Traffic map configurations apply to all ports in a LAG.

There can be, at the most, 16 entries in the Priority Group table. Eight of the entries are Strict Priority entries with a Priority Group ID of 15.0 to 15.7 and eight are user-definable entries with a Priority Group ID of 0-7.

See Table 31 for an example of priority group configuration.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.

3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

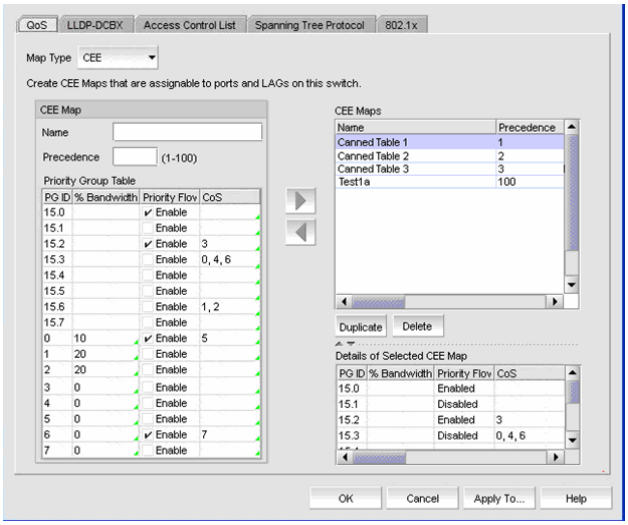


FIGURE 92 **QoS, Create CEE Map dialog box**

4. Select CEE from the **Map Type** list.
5. Configure the following CEE Map parameters in the **CEE Map** table:
   - **Name** - Enter a name to identify the CEE map.
   - **Precedence** - Enter a value between 1 - 100. This number determines the map's priority.
   - **Priority Flow Control** check box - Check to enable priority flow control on individual priority groups.
   - **CoS** - Enter a Class of Service value to correspond to the Priority Group ID rows. All of the eight CoS values (0-7) must be used in a CEE map. Duplicate CoS values in two or more priority groups are not allowed.

     NOTE
     You can only edit CoS fields that are displayed with a green tick mark.

     % Bandwidth *(optional)* - Enter a bandwidth value for priority group (PG) IDs 0-7. You must map each CoS to at least one of the PG IDs. Use a comma and a space to separate multiple CoS values, as shown in Figure 92.

     Note the following points:

     - You cannot define a bandwidth percentage for Strict Priorities (PG ID 15.0 - 15.7). The total % Bandwidth for PG ID 15.0-15.7 must equal 0%.
     - If you set a CoS value to one or more of the PG IDs 0-7 and you set Priority Flow Control to **Enabled**, you must also enter a non-0% bandwidth percentage. The total % Bandwidth must equal 100%.
     - For PG IDs 0-7 that do not have an assigned CoS value or PFC enabled, the % Bandwidth must be 0%.

6. Click the right arrow button to add the map to the CEE Maps table.
7. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

Editing a CEE map

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.
4. Select a CEE Map from the **CEE Maps** table, and click the left arrow button to load its values to the left pane. The fields are now editable.
5. Keep the same CEE Map name and modify the following values, as required. See Table 31 for an example of priority group configuration.
   - **Precedence** - Enter a value between 1 - 100. This number determines the map's priority.
   - **% Bandwidth** - Enter a bandwidth value for priority group IDs 0-7. The total of all priority groups must equal 100%.
   - **Priority Flow Control** check box - Check to enable priority flow control on individual priority groups.
   - **CoS** - Enter a Class of Service value to correspond to the Priority Group ID rows. Each CoS must be mapped to at least one of the Priority Group IDs (0-7), separated with a comma and a space, as shown in Figure 92.
6. Click the right arrow button to re-add the map to the CEE Maps table.

   If the CEE Map already exists, an overwrite message displays.
7. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

Deleting a CEE map

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select a CEE Map that you want to delete from the **CEE Maps** table.
5. Click **Delete**.

   The Delete confirmation dialog displays.

6. Click **Yes** to confirm.

   The CEE Map row is removed from the table.

7. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

Duplicating a CEE map

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select a CEE Map that you want to duplicate from the **CEE Maps** table.
5. Click **Duplicate**.

   An input dialog pops up if the duplicated map exceeds the maximum length.

   If the map does not exceed the maximum length, a copy of the selected row is created with the name <*name of CEE map*>_copy.

6. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Assigning a CEE map to a port or link aggregation group

A port can have either a CEE map or a Traffic Class map assigned to it, but it cannot have both.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a port or LAG, and click **Edit**.
3. Click the **QoS** tab on the **Edit Port** dialog box.

   The **QoS** dialog box displays.

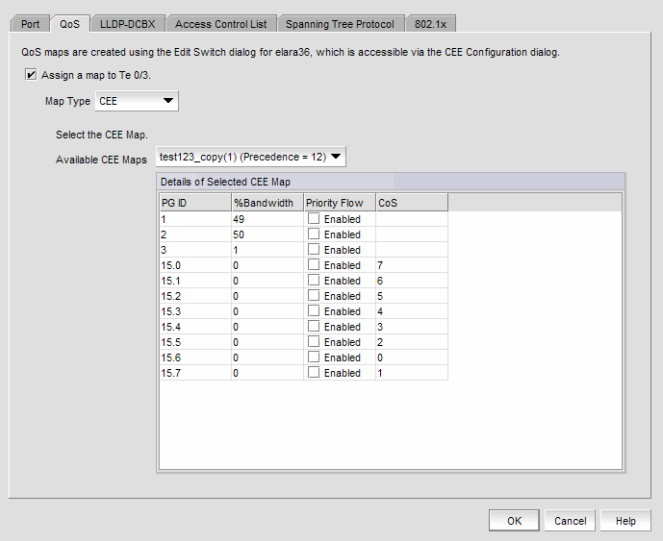


FIGURE 93 QoS, Assign a CEE Map to a port dialog box

4. Click the **Assign a map to <port name>** check box.

   If you do not enable this check box, all QoS edit features are disabled.

5. Select **CEE Map** in the **Map Type** list.
6. Select a CEE Map in the **Available CEE Maps** list.
7. Click **OK** to commit the map assignment.

   The **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

Creating a traffic class map

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select **Traffic Class** from the **Map Type** list.
5. Name the Traffic Class map.
6. Click the Traffic Class cell in a CoS row and directly enter a value from 0-7. You can leave the cell empty to indicate zero (0).
7. Click the right arrow button to add the map to the **Traffic Class Maps** table.

   If the name of the Traffic Class map already exists, an overwrite warning message displays. Click **Yes** to overwrite the existing Traffic Class map.

8. Click **OK** if the Traffic Class map does not already exist.

   The **CEE Confirmation and Status** dialog box displays.

9. Review the changes carefully before you accept them.
10. Click **Start** to apply the changes, or click **Close** to abort the operation.

Editing a traffic class map

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select a Traffic Class Map from the **Traffic Class Maps** table, and click the left arrow button to load its values to the left pane. The fields are now editable.
5. Keep the same Traffic Class Map name and modify the values, as required.
6. Click the right arrow button to re-add the map to the Traffic Class Maps table.
7. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

Deleting a traffic class map

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select a Traffic Class Map that you want to delete from the **Traffic Class Maps** table.
5. Click **Delete**.

   The **Delete confirmation** dialog displays.

6. Click **Yes** to confirm.

   The Traffic Class Map row is removed from the table.

7. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

Duplicating a traffic class map

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select a Traffic Class Map that you want to duplicate from the **Traffic Class Maps** table.
5. Click **Duplicate**.

   An input dialog pops up if the duplicated map exceeds the maximum length.

   If the map does not exceed the maximum length, a copy of the selected row is created named <*name of Traffic Class Map*>_copy.

6. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Assigning a traffic class map to a port or link aggregation group

You can assign a Traffic Class map to a port or ports under the LAG; however, a port does not *require* a Traffic Class map be assigned to it. A port can have either a CEE map or a Traffic Class map assigned to it, but it cannot have both.

NOTE
You cannot configure QoS or LLDP-DCBX on a LAG.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a port or LAG, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

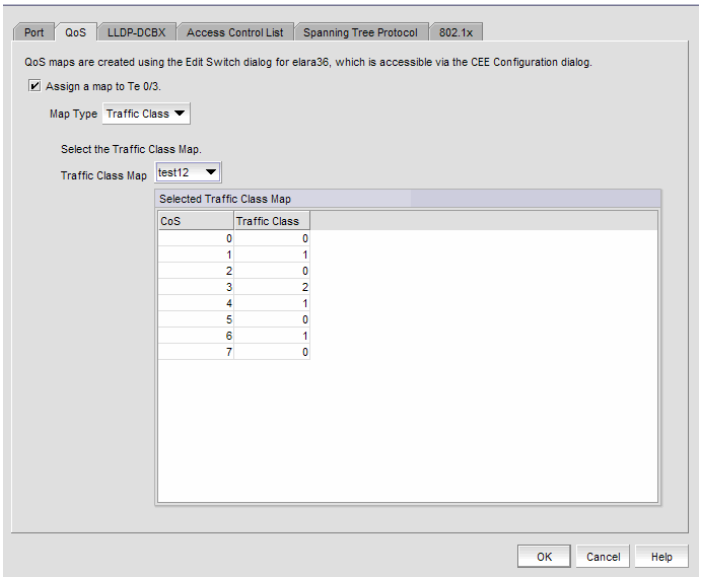


FIGURE 94 QoS, assign a traffic class map to a port dialog box

4. Click the **Assign a map to <port name>** check box.
5. Select **Traffic Class** in the **Map Type** list.
6. Select a Traffic Class Map in the **Traffic Class Map** list.
7. Click **OK** to commit the map assignment.

   The **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

LLDP-DCBX configuration

Link Layer Discovery Protocol (LLDP) provides a solution for the configuration issues caused by increasing numbers and types of network devices in a LAN environment, because, with LLDP, you can statically monitor and configure each device on a network.

Data Center Bridging Capability Exchange Protocol (DCBX) enables Enhanced Ethernet devices to discover whether a peer device supports particular features, such as Priority Flow Control or Class of Service (CoS). In a Converged Enhanced Ethernet (CEE) environment, LLDP is enhanced with DCBX protocol to further share or change the configured CEE enhancements. You must enable the DCBX protocol and configure certain parameters in order to effectively utilize the benefits of a converged network.

Using the **LLDP-DCBX** dialog box, you can create and manage LLDP profiles and assign a LLDP profile to a port or link aggregation group (LAG).

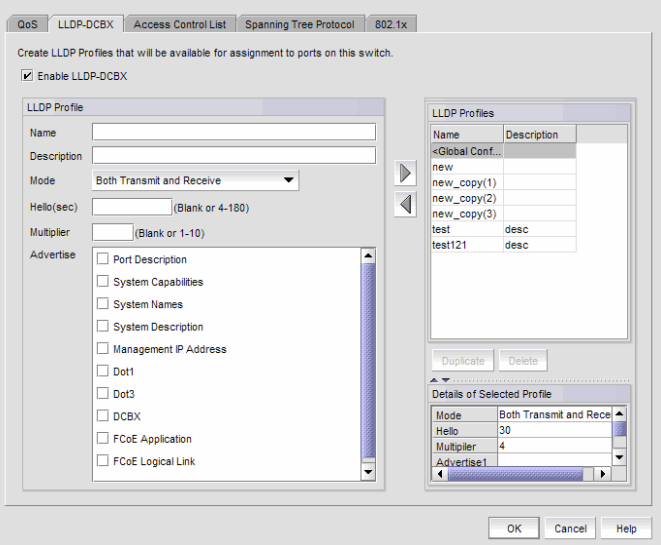


FIGURE 95 LLDP-DCBX dialog box (switch level)

Adding an LLDP profile

When LLDP is disabled on the switch, a yellow banner displays on the **LLDP-DCBX** dialog box, indicating that LLDP-DCBX is not only disabled on the switch, it is also disabled for all ports and LAGs on the switch.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.

   The **LLDP-DCBX** dialog box displays.

4. Click the **Enable LLDP-DCBX** checkbox.
5. Configure the LLDP Profile parameters:
   - **Name** - Type a name for the LLDP profile. If the name of the LLDP profile already exists on the switch, an overwrite warning displays. The overwrite warning does not apply to the <Global Configuration> name, because that name cannot be edited.
   - **Description** - Type a meaningful description of the LLDP profile.
   - **Mode** - Select a mode from the list: Tx (transmitted) or Rx (received).
   - **Hello** - Enter a hello interval time for the bridge. The value range is 4-180 and the default value is 30.
   - **Multiplier** - Enter a multiplier. The value range is 1-10 and the default is 4.
   - **Advertise** - Check the profile parameters that you want to display as part of the LLDP profile:
     - Port description - The user-configured port description.
     - System name - The user-configured name of the local system.
     - System capabilities - The system capabilities running on the system.
     - System description - The system description containing information about the software running on the system.
     - Management IP address - The IP management address of the local system.
     - Dot 1..Dot 3 -
     - DCBX - The DCBX profiles.
     - FCoE application - The FCoE application feature.
     - FCoE logical link - The logical link level for the SAN network.
6. Click the right arrow button to move the newly created profile into the DBCX Profiles table.
7. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

Editing an LLDP profile

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.

   The **LLDP Profile** dialog box displays.

4. Select an LLDP Profile in the **LLDP Profile** table.

   NOTE
   You can edit the <Global Configuration> profile. You cannot, however, delete, rename, or duplicate global configurations.

5. Click the left arrow to load the LLDP Profile's values to the left pane.
6. Modify the values, as described in "Adding an LLDP profile" on page 292. You are not allowed to modify the LLDP Profile's name.
7. Click the right arrow to update the LLDP Profile parameters.
8. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

9. Review the changes carefully before you accept them.
10. Click **Start** to apply the changes, or click **Close** to abort the operation.

Deleting an LLDP profile

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.

   The **LLDP Profile** dialog box displays.

4. Select an existing LLDP Profile from the **LLDP Profiles** table in the upper right pane.

   NOTE
   You cannot delete <Global Configurations>. You can, however, edit global configurations. For more information, see "Editing an LLDP profile" on page 293

5. Click **Delete**.

   A confirmation dialog displays.

6. Click **Yes** to confirm you want to delete the LLDP profile.

   The **LLDP Profile** table row is removed.

7. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

Duplicating an LLDP profile

When you duplicate an LLDP profile, you also duplicate the parameters that belong to that LLDP Profile.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.

   The **LLDP Profile** dialog box displays.

4. Select an existing LLDP Profile from the **LLDP Profiles** table in the upper right pane.

   NOTE
   You cannot duplicate <Global Configurations>. You can, however, edit global configurations. For more information, see "Editing an LLDP profile" on page 293.

5. Click **Duplicate**.

   An input dialog pops up if the duplicated map exceeds the maximum length.

   If the map does not exceed the maximum length, a copy of the LLDP profile displays in the LLDP Profiles table.

6. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Assigning an LLDP profile to a port or ports in a LAG

You create LLDP profiles using the **Edit Switch** dialog box, which you access from the **CEE Configuration** dialog box. Global configuration parameters, which is the default selection, are displayed in the Assigned Profile table shown in Figure 96.

NOTE
When LLDP is disabled on the switch, a yellow banner displays on the **LLDP-DCBX** dialog box, indicating that LLDP-DCBX is not only disabled on the switch, it is also disabled for all ports and LAGs on the switch.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a port or link aggregation group (LAG), and click **Edit**.

3. Click the **LLDP-DCBX** tab on the **Edit Port/Edit LAG** dialog box.

   The **Assign an LLDP profile to <port name>** dialog box displays.

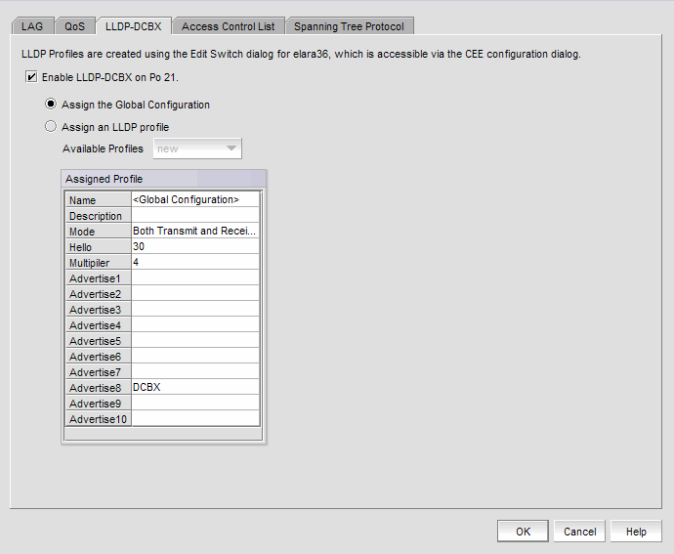


FIGURE 96 **Assign an LLDP profile dialog box**

4. Click **Assign an LLDP profile to <port name>** button to enable the feature.

   NOTE
   Assign the Global Configuration is the default. The **Available Profiles** list is disabled if global configuration is selected. In addition, the **Assign an LLDP profile** button is disabled if no LLDP profiles exist on the switch.

5. Select an LLDP profile from the **Available Profiles** list.

6. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them. The port you selected on the **CEE Configuration** dialog box should now be assigned to the profile you selected from the **Available Profiles** list.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Access Control List configuration

Access control lists (ACL) are sequential lists consisting of permit and deny rules. They are either Layer 3 (IP)- or Layer 2 (MAC)-specific. You can configure multiple access lists and rules and store them in the configuration.

Some of the benefits of ACLs include the following:

- ACLs provide a measure of security.
- ACLs save network resources by reducing traffic.
- ACLs block unwanted traffic and users.
- ACLs reduce the chance of attacks.

You create an ACL on a switch and then you can apply the configuration to ports, and link aggregation groups (LAGs) on that switch.

Adding an ACL to a switch

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **Access Control List** tab on the **Edit Switch** dialog box.

   The **Access Control List** dialog box displays.

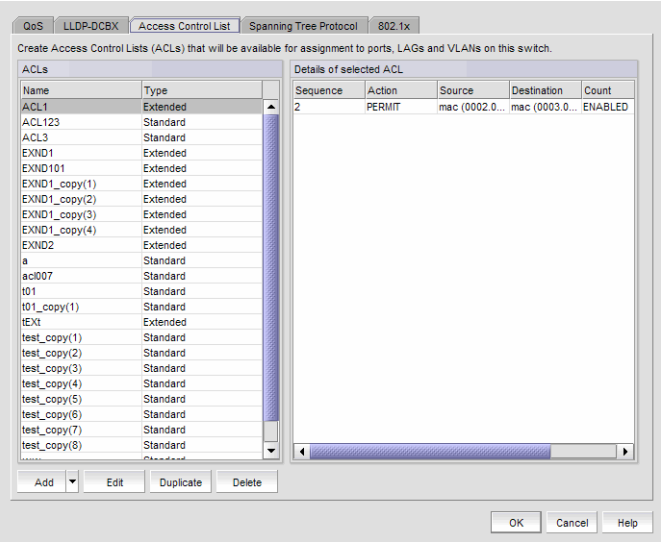


FIGURE 97 Access Control List dialog box

4. Click **Add** and select **Standard** or **Extended** from the **Add** list.

   The **Add Extended Access Control List** includes all the Standard ACL features plus two additional features: Destination and Ether Type. The ACL parameters are described below.

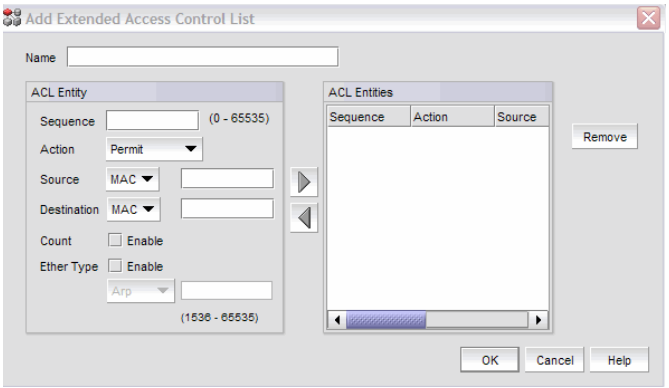


FIGURE 98 Add Extended Access Control List dialog box

5. Configure the following Access Control List parameters.

NOTE
You cannot duplicate Action and Source parameters in an existing Standard ACL. You cannot duplicate Action, Source, Destination, and Ether Type parameters in an existing Extended ACL.

- **Sequence** - The sequence number that tracks all the ACL entities defined globally in the system. If you assign a Sequence number that is the same as an existing ACL Entity, an overwrite warning displays. After the overwrite operation, the system again checks for duplicates, then it creates the new ACL entity.

- **Action** - Select Permit or Deny from the list.

  NOTE
  If **Action = Deny** is selected for any ACL entity, an informational dialog displays with the following message: “This ACL entity will stop all traffic to the port or LAG on which this ACL is assigned.”

- **Source** - Enter the media access control (MAC) address where the packets originate. **Mask** is the subnet mask of the source MAC address. If you select “Any” from the **Source** list, the text box is cleared and disabled and the subnet mask is not applicable.

  In the **Extended ACL** dialog box, you can select **Host** from the **Source** list, in addition to **MAC** or **Any**. If you select **Host** from the list, enter the host name where the packets originate.

- **Destination** - Enter the user-supplied packet destination MAC address. **Mask** is the packet subnet mask of the packet destination MAC address. If you select “Any” from the **Destination** list, the text box is cleared and disabled and the subnet mask is not applicable.

  In the **Extended ACL** dialog box, you can select **Host** from the **Destination** list, in addition to **MAC** or **Any**. If you select **Host** from the list, enter the host name of the packet destination.

- **Count** - Instructs the system to maintain a counter.
- **Ether Type -** Specifies the Ethernet protocol being transferred in the Ethernet frame. Only one of the following Ether types is supported at a time.
  - Custom - Enter a value between the range of 1536 and 65535.
  - Arp
  - FCoE
  - IPv4

6. Click the right button to add the ACL entity to the **ACL Entities** table.
7. Click **OK** to close the dialog box. The newly-added ACL displays in the **ACL Entities** table.

   If the name of the ACL already exists (duplicate Standard or Extended ACL names cannot exist), an overwrite warning message displays. Click **Yes** to overwrite the existing ACL.

   If the name of the ACL does not already exist, the **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click the **Start** button to apply the changes, or click **Close** to abort the operation.

   You can now assign the ACL to ports or link aggregation groups (LAGs) on the switch.

Editing the parameters of an ACL

You cannot change the name of the ACL (Standard or Extended) after you have created the ACL on the switch.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **Access Control List** tab on the **Edit Switch** dialog box.

   The **Access Control List** dialog box displays.

4. Select an ACL row in the **ACLs** table and click **Edit**.
5. Modify the ACL parameters, as required, using the parameter descriptions in "Adding an ACL to a switch" on page 296.
6. Click **OK** to commit the ACL parameter changes.

   The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Deleting an ACL

When you delete an ACL from the **ACLs** table, you are given the option to also remove the profile from the entities where it is currently associated.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **Access Control List** tab on the **Edit Switch** dialog box.

   The **Access Control List** dialog box displays.

4. Select the ACL that you want to delete from the **ACLs** table.
5. Click **Delete**.

   The selected ACL is removed from the ACLs table.

6. Click **OK** to commit the ACL parameter changes.

   The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Duplicating an ACL profile

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **Access Control List** tab on the **Edit Switch** dialog box.

   The **Access Control List** dialog box displays.

4. Select the ACL that you want to duplicate from the **ACLs** table.
5. Click **Duplicate**.

   An input dialog pops up if the duplicated map exceeds the maximum length.

   If the map does not exceed the maximum length, a copy of the selected ACL is added to the ACLs table.

6. Click **OK** to commit the ACL parameter changes.

   The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Assigning an ACL to a port or link aggregation group

An access control list (ACL) cannot be assigned to a port when the port is a member of a link aggregation group (LAG). An ACL can be assigned to a LAG, however.

NOTE
The ports and the ports in a link aggregation group (LAG) for the selected switch must be in Layer 2 (L2) mode. If the ports or ports in a LAG are not in L2 mode, the ACL parameters are disabled.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a port or LAG, and click **Edit**.
3. Click the **Access Control List** tab on the **Edit Port/Edit LAG** dialog box.

   The **Access Control List** dialog box displays.

4. Click the **Assign Access Control List to <port name>** checkbox.

   You can unassign an ACL by deselecting the **Assign an ACL to <port_name>** checkbox.

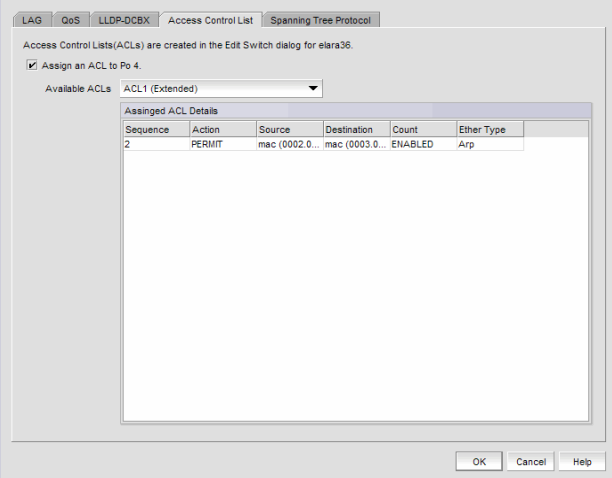


FIGURE 99 **Assign ACL to port dialog box**

5. Select an ACL from the **Available ACLs** list.

   The ACL name is suffixed with its type (standard or extended) in parentheses; for example, Human Resources (Extended). The details of the selected ACL are displayed in the Assigned ACL Details table, shown in Figure 99.

6. Click **OK** to commit the assign the ACL to the port or LAG.

   The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Spanning Tree Protocol configuration

You can configure Spanning Tree Protocol (STP) when editing a LAG, but not when you are adding a LAG. The 8 Gbps 16-FC-ports, 10 GbE 8-Ethernet Port supports the following types of STP:

- Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RSTP) - Provides for faster spanning tree convergence after a topology change. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.
- Multiple Spanning Tree Protocol (MSTP) - Provides support for virtual LANs (VLANs). This "per-VLAN" Multiple Spanning Tree Protocol configures a separate spanning tree for each VLAN group and blocks the links that are redundant within each spanning tree.

See "Spanning Tree Protocol policy" on page 273 for general information about Spanning Tree Protocol.

Enabling Spanning Tree Protocol

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **Spanning Tree Protocol** tab on the **Edit Switch** dialog box.

   The **Enable Spanning Tree Protocol** dialog box displays.

4. Configure the Spanning Tree parameters, which are described in "Setting Spanning Tree parameters for a switch" on page 303.
5. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

6. Review the changes carefully before you accept them.
7. Click **Start** to apply the changes, or click **Close** to abort the operation.

Setting Spanning Tree parameters for a switch

You cannot configure Spanning Tree Protocol (STP) when adding a new LAG. STP can be configured only after the LAG has been added to the switch.

NOTE
The ports and the ports in a link aggregation group (LAG) for the selected switch must be in Layer 2 (L2) mode. If the ports or ports in a LAG are not in L2 mode, Spanning Tree Protocol is disabled and the STP parameters are disabled as well.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **Spanning Tree Protocol** tab on the **Edit Port** dialog box.

   The **Enable Spanning Tree Protocol** dialog box displays.

4. Click the **Enable Spanning Tree Protocol** check box to enable STP, and click **OK**.

   The **Spanning Tree Protocol** dialog box displays.

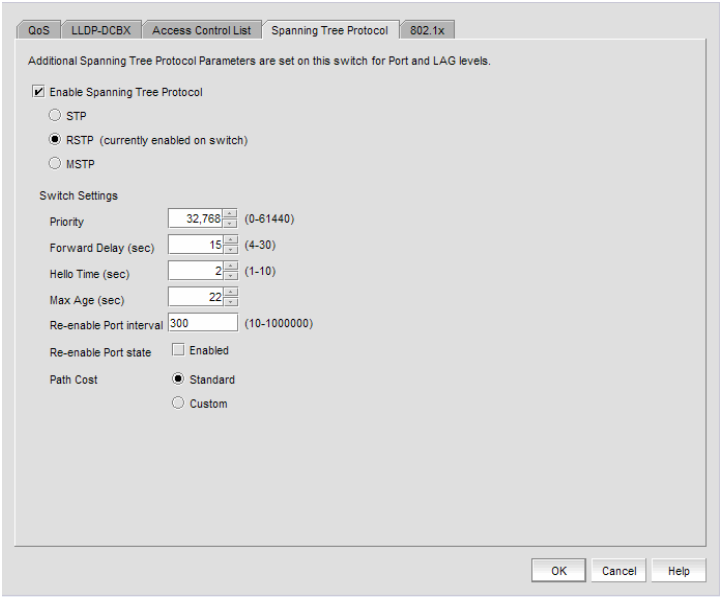


FIGURE 100 Spanning Tree Protocol dialog box, STP and RSTP

NOTE
(currently enabled on switch) indicates which STP mode is configured on the switch.

5. Configure the following Spanning Tree Protocol parameters:

   - **Priority** - The bridge priority. The value range is 0-61440 and the default value is 32768. The value must be in increments of 4096.
   - **Mode** - The spanning tree protocol mode. Options include Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP).
   - **Forward Delay (sec)** - The forward delay for the bridge. The value range is 4-30 seconds and the default value is 15.
   - **Hello Time (sec)** - The hello interval time for the bridge. The value range is 1-10 and the default value is 2.
   - **Maximum Age (sec)** - The maximum time to listen in seconds. The value range is 6-40 and the default is 20 seconds. This feature is not available if running in MSTP mode.

     The maximum age has a range of [2 x Hello Time +1] to [2 x Forward Delay - 1]. If you specify a Maximum Age value that exceeds this range, an error message displays.
   - **Re-enable Port Interval** - The interval after which the port will be enabled. The value range is 10-1000000 and the default is 300.
   - **Re-enable Port State** - Enables or disables the timeout mechanism for the port to be enabled back.
   - **Path Cost** - Sets the path cost behavior. Options include Standard and Custom.

   You can set additional STP parameters, listed below, on the selected switch if MSTP Spanning Tree Protocol is enabled, as shown in Figure 101.

   - **Cisco Interop** - Enables or disables Cisco interoperability.
   - **Tx Hold Count** - Select the transmit hold count for the bridge. The value range is 1-10.
   - **Max Hops -** Specify the number of hops in a region before the Bridge Protocol Data Units (BPDU) are discarded and the information held for a port is aged. The hop count determines when to trigger a reconfiguration. The value range is 1-40 and the default is 20.
   - **Region -** The Multiple Spanning Tree (MST) region.
   - **Revision -** The revision number for the configuration. The value range is 0-255 and the default is 0.

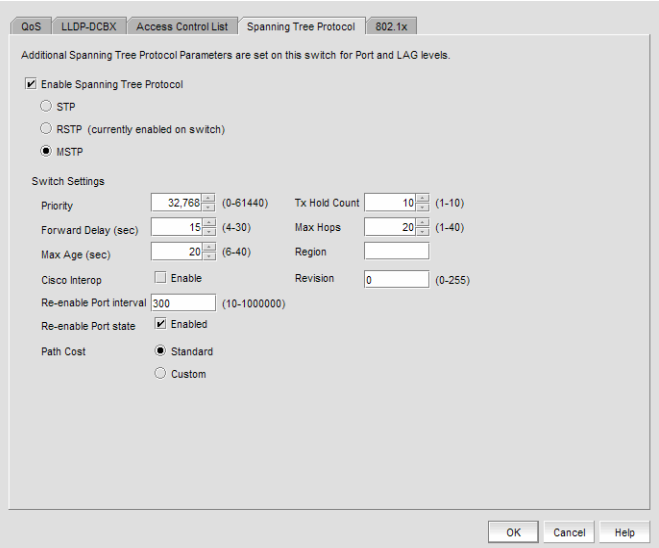


FIGURE 101 **Spanning Tree Protocol dialog box, MSTP**

6. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

STP configurable parameters at the port or LAG level

You cannot configure Spanning Tree Protocol (STP) when adding a new LAG. STP can be configured only after the LAG has been added to the switch.

NOTE
When STP is disabled on the switch, a yellow banner displays on the dialog box, indicating that STP is not only disabled on the switch, it is also disabled for all ports and LAGs on the switch. The yellow banner also displays when a LAG or port is not in L2 mode.

Figure 102 shows the Spanning Tree Protocol (STP) parameters that are configurable at the port or LAG level.

The ports and the ports in a link aggregation group (LAG) for the selected switch must be in Layer 2 (L2) mode. If the ports or ports in a LAG are not in L2 mode, Spanning Tree Protocol is disabled and the STP parameters are disabled as well.

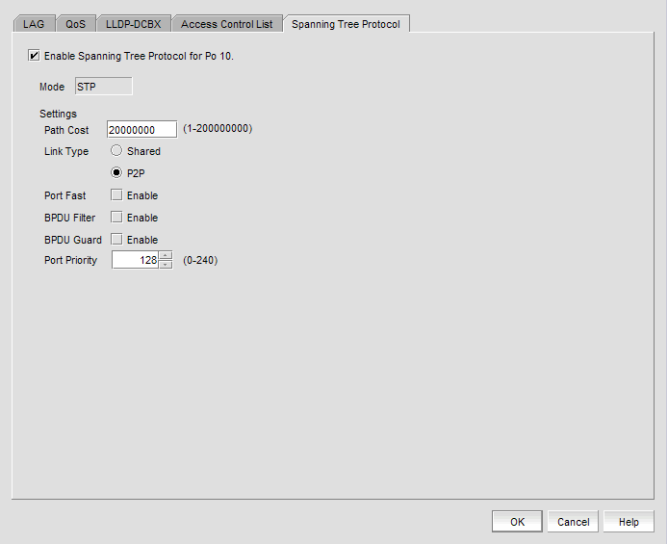


FIGURE 102 Spanning Tree Protocol dialog box, STP and RSTP

You can configure the following Spanning Tree Protocol parameters.

- **Mode** - The spanning tree protocol mode.
- **Path Cost** - The port's path cost. The value range is 1 - 2000000000.
- **Link Type** - The link type for STP. Valid values are Shared or P2P.
- **Port Fast** - Enables an interface to move directly to forward on link up. Valid values are Enable or Disable, applicable only to STP.
- **BPDU Filter** - Sets the portfast filter for the Bridge Protocol Data Units (BPDU). Valid values are Enable or Disable.
- **BPDU Guard** - Guards the port against the reception of BPDUs. Valid values are Enable or Disable.
- **Port Priority -** Port priority for MSTP. The value range is 0-240.

802.1x authentication

802.1x is a standard authentication protocol that defines a client-server-based access control and authentication protocol. 802.1x restricts unknown or unauthorized clients from connecting to a LAN through publicly accessible ports.

You must configure parameters for a port or a link aggregation group (LAG) once a port has been enabled for 802.1x authentication. See Setting 802.1x parameters for a port for more information.

NOTE
When 802.1x is disabled on the switch, a yellow banner displays on the dialog box, indicating that 802.1x is not only disabled on the switch, it is also disabled for all ports on the switch.

Enabling 802.1x authentication

802.1x authentication is enabled or disabled globally on the switch using the **Edit Switch** dialog box. You can configure 802.1x authentication when editing a LAG, but not when you are adding a LAG.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a port or LAG, and click **Edit**.
3. Click the 802.1x tab on the **Edit Port** dialog box.

   The **Enable 802.1x** dialog box displays.

4. Click the **Enable 802.1x** check box to enable 802.1x authentication, and click **OK**.

   The **802.1x** dialog box displays.

5. Configure the 802.1x parameters, which are described in "Setting 802.1x parameters for a port" on page 308.
6. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

Disabling 802.1x

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a port or LAG, and click **Edit**.
3. Click the 802.1x tab on the **Edit Port** dialog box.

   The 802.1x dialog box displays.

4. Clear the **Enable 802.1x** check box to disable 802.1x authentication.
5. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.

6. Review the changes carefully before you accept them.
7. Click **Start** to apply the changes, or click **Close** to abort the operation.

Setting 802.1x parameters for a port

The 802.1x parameters can be configured whether the feature is enabled on the switch or a port. The default parameters are initially populated when 802.1x is enabled on a port, but you can change the default values as required.

1. Select **Configure > CEE Switch > CEE** from the menu bar.

   The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a port, and click **Edit**.
3. Click the 802.1x tab on the **Edit Port** dialog box.

   The **Enable 802.1x** dialog box displays.

4. Click the **Enable 802.1x** check box to enable 802.1x authentication, and click **OK**.

   The **802.1x** dialog box displays.

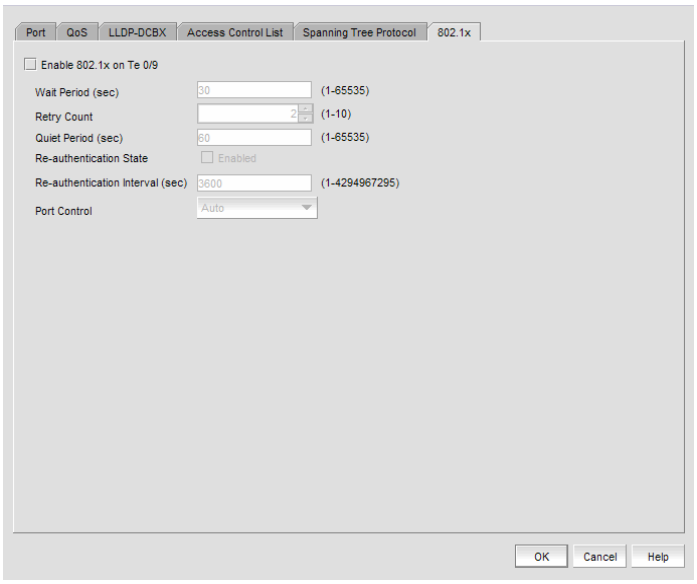


FIGURE 103 802.1x dialog box

6. Configure the following 802.1x parameters:
   - **Wait Period** - The number of seconds the switch waits before sending an EAP request. The value range is 15 to 65535 seconds. The default value is 30.
   - **Retry Count** - The maximum number of times that the switch restarts the authentication process before setting the port to an unauthorized state. The value range is 1 to 10. The default value is 2.
   - **Quiet Period** - The number of seconds that the switch remains in the quiet state after a failed authentication exchange with the client. The value range is 1 to 65535 seconds. The default value is 60.
   - **Re-authentication State** - Enable or disable the periodic re-authentication of the client. The default is Disable.
   - **Re-authentication Interval** - The number of seconds between re-authentication attempts. The value range is 1 to 4294967295. The default value is 3600 seconds. This feature is not dependent on the re-authentication state being enabled.
   - **Port Control** - Select an authorization mode from the list to configure the ports for authorization. Options include auto, force-authorized, or force-unauthorized and the default value is auto.
7. Click **OK**.

   The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

Virtual FCoE port configuration

The 8 Gbps 16-FC-ports, 10 GbE 8-Ethernet Port has the following configuration features:

- 24 10 Gbps Ethernet ports, which can be enabled for FCoE traffic.
- One-to-one mapping of FCoE ports with 10 Gbps Ethernet ports.
- Eight 8 Gbps FC ports.
- 24 internal FCoE ports, which provide the Ethernet-to-FC bridging capability. You can enable or disable each FCoE trunk individually.
- Each of the FCoE ports can be configured as an E_Port or an F_Port.

Viewing virtual FCoE ports

1. Select **Configure > CEE Switch > FCoE** from the menu bar.

   The **FCoE Configuration** dialog box displays.

2. Select the **Virtual FCoE Ports** tab.

   The **Virtual FCoE Ports** tab displays.

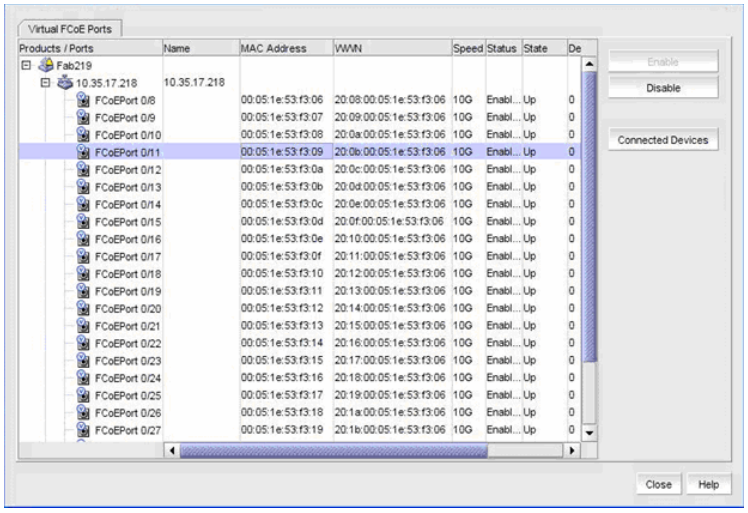


FIGURE 104 Virtual FCoE Ports dialog box

The **Virtual FCoE Configuration** dialog box enables you to perform the following tasks:

- Click **Enable** to enable a selected virtual FCoE port for CEE configuration.
- Click **Disable** to disable a selected virtual FCoE port from CEE configuration.
- View a list of FCoE virtual ports and to what they are directly connected.
- Display performance statistics for FCoE ports.

Instructions for performing the Virtual FCoE configuration tasks are detailed in the following sections:

3. Click **Close** to close the dialog box.

Clearing a stale entry

A stale entry is a device that logged in and logged off but, because a port went down after an FLOGI was received, the device failed to receive the message. The entry in the **FCoE Connected Devices** table becomes stale and you must clear it manually.

1. Select a virtual FCoE port from the **FCoE Configuration** dialog box and click **Connected Devices**.

   The **Connected Devices** dialog box displays.

2. Select one or more rows from the **Connected Devices** table and click **Disconnect**.

   The **CEE Confirmation and Status** dialog displays.

3. Click **OK**.

   The selected connected device should be cleared from the switch cache and from the table. Note, however, that the connected devices might still be active and this operation could potentially stop traffic between the connected devices and the switch.

4. Review the changes carefully before you accept them.

5. Click **Start** to apply the changes, or click **Close** to abort the operation.

   On closing the CEE Confirmation and Status dialog box, the **FCoE Configuration** Dialog refreshes the data and the latest information about the FCoE ports are displayed.

Chapter

12

Encryption configuration

In this chapter

- Gathering information 314
- Encryption user privileges 315
- Encryption Center features 316
- Smart card usage 316
- Viewing and editing switch encryption properties 320
- Viewing and editing group properties 324
- Encryption Targets dialog box 333
- Creating a new encryption group 336
- Adding a switch to an encryption group 344
- Creating high availability (HA) clusters 347
- Adding encryption targets 350
- Configuring hosts for encryption targets 357
- Adding Target Disk LUNs for encryption 358
- Adding Target Tape LUNs for encryption 361
- Configuring encrypted storage in a multi-path environment 362
- Master keys 363
- Zeroizing an encryption engine 373
- Tracking Smart Cards 375

Gathering information

Before you use the encryption setup wizard for the first time, you should also have a detailed configuration plan in place and available for reference. The encryption setup wizard assumes the following:

- You have a plan in place to organize encryption devices into encryption groups.
- If you want redundancy and high availability in your implementation you have a plan to create high availability (HA) clusters of two encryption switches or blades to provide failover support.
- All switches in the planned encryption group are interconnected on an I/O synch LAN.
- The management ports on all encryption switches and DCX CPs that have encryption blades installed have a LAN connection to the SAN management program, and are available for discovery.
- A supported key management appliance is connected on the same LAN as the encryption switches, DCX CPs, and the SAN Management program.
- An external host is available on the LAN to facilitate certificate exchange.
- Switch KAC certificates have been signed by a Certificate Authority (CA), and stored in a known location.
- Key management system (key vault) certificates have been obtained and stored in a known location.

Encryption user privileges

In the Management application, resource groups are assigned privileges, roles, and fabrics. Privileges are not directly assigned to users; users get privileges because they belong to a role in a resource group. A user can only belong to one resource group at a time.

The Management application provides three pre-configured roles:

- Storage encryption configuration.
- Storage encryption key operations.
- Storage encryption security.

Table 32 lists features and the associated roles with read/write access and read-only access.

TABLE 32 Role-based access control privileges and descriptions

Privilege	Read-Only	Read/Write
Storage Encryption Configuration	Disables all functions from the **Encryption Center** dialog box except view.	Enables the following functions from the **Encryption Center** dialog box: • Launch the Configure Encryption dialog. • View switch, group, or engine properties. • View the Encryption Group Properties Security tab. • View encryption targets, hosts, and LUNs. • Create a new encryption group or add a switch to an existing encryption group. • Edit group engine properties (except for the Security tab) • Add targets. • Select encryption targets and LUNs to be encrypted or edit LUN encryption settings. • Edit encryption target hosts configuration. • Change routing mode on an encrypyion engine.
Storage Encryption Key Operations	Disables all functions from the **Encryption Center** dialog box except view.	Enables the following functions from the **Encryption Center** dialog box: • Launch the Configure Encryption dialog. • View switch, group, or engine properties, • View the Encryption Group Properties Security tab. • View encryption targets, hosts, and LUNs. • Initiate manual LUN re-keying. • Enable and disable an encryption engine. • Zeroize an encryption engine. • Restore a master key. • Edit key vault credentials.
Storage Encryption Security	Disables all functions from the **Encryption Center** dialog box except view.	Enables the following functions from the **Encryption Center** dialog box: • Launch the Configure Encryption dialog. • View switch, group, or engine properties. • View encryption targets, hosts, and LUNs. • Create a master key. • Backup a master key. • Enable encryption functions after a power cycle. • View and modify settings on the Encryption Group Properties Security tab (quorum size, authentication cards list and system card requirement). • Establish link keys for LKM key managers.

Encryption Center features

The **Encryption Center** dialog box (Figure 105) is the single launching point for all encryption-related configuration in the Management application. It also provides a table that shows the general status of all encryption-related hardware and functions at a glance.

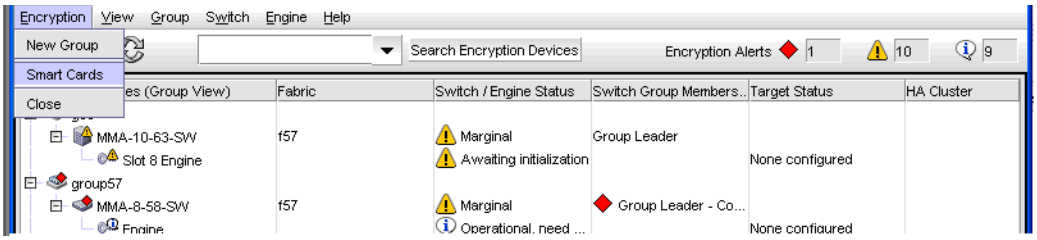


FIGURE 105 Encryption Center dialog box

The **Encryption Center** dialog box differs from the previous **Configure Encryption** dialog box. The buttons at the bottom of the dialog box are replaced with menus that are selected from a menu bar, or alternatively, by right-clicking an item in the table.

Smart card usage

Smart Cards are credit card-sized cards that contain a CPU and persistent memory. Smart cards can be used as security devices. With Brocade encryption switches, smart cards can be used to do the following:

- Control user access to the Management application security administrator roles.
- Control activation of encryption engines.
- Securely store backup copies of master keys.

Smart card readers provide plug-and-play interface to read and write to a smart card. The following smart card readers are supported:

- GemPlus GemPC USB

  http://www.gemalto.com/readers/index.html
- SCM MicrosystemsSCR331

  http://www.scmmicro.com/security/view_product_en.php?PID=2

See the following procedures for instructions about how to configure a Smart Card:

- "Registering authentication cards from a card reader" on page 317
- "Registering system cards from a card reader" on page 319
- "Saving a master key to a smart card set" on page 367
- "Restoring a master key from a smart card set" on page 371

Registering authentication cards from a card reader

When authentication cards are used, one or more authentication cards must be read by a card reader attached to a Management application PC to enable certain security sensitive operations. These include the following:

- Master key generation, backup, and restore operations.
- Replacement of authentication card certificates.
- Enabling and disabling the use of system cards.
- Changing the quorum size for authentication cards.
- Establishing a trusted link with the NetApp LKM key manager.

To register an authentication card or a set of authentication cards from a card reader, have the cards physically available. Authentication cards can be registered during encryption group or member configuration when running the configuration wizard, or they can be registered using the following procedure.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select an encryption group, and select **Security Settings**.

3. Select the **Quorum Size**.

   The quorum size is the minimum number of cards necessary to enable the card holders to perform the security sensitive operations listed above. The maximum quorum size is five cards. The actual number of authentication cards registered is always more than the quorum size, so if you set the quorum size to five, for example, you will need to register at least six cards in the subsequent steps.

   NOTE
   Ignore the **System Cards** setting. Refer to "Enabling or disabling the system card requirement" on page 320 for information on its usage.

4. Click **Next**.

   The **Register Authentication Cards** dialog is displayed. This dialog include a table that shows all registered authentication cards.

5. Select **Register from Card Reader** to register a new card.

   The **Add Authentication Card** dialog box is displayed.

6. Insert a smart card into the card reader. Be sure to wait for the card serial number to appear, and then enter card assignment information, as directed.

7. Click **OK**.

8. Wait for the confirmation dialog box indicating initialization is done, and click **OK**.

   The card is added to the **Registered Authentication Cards** table on the **Authentication Cards** dialog box.

9. Repeat steps 7 through 10 until you have registered all the cards, and they all display in the **Registered Authentication Cards** table on the **Authentication Cards** dialog box. Remember that you need to register the number selected as the quorum size plus one.

Registering authentication cards from the database

Smart cards that are already in the Management program's database can be registered as authentication cards.

1. From the **Register Authentication Cards** dialog box, select **Register from Archive**.

   The **Authentication Cards** dialog box displays, showing a list of smart cards in the database.

2. Select the card from the table, and click **OK**.
3. Wait for the confirmation dialog box indicating initialization is done, and click **OK**.

   The card is added to the **Registered Authentication Cards** table.

De-registering an authentication card

Authentication cards can be removed from the database and the switch by de-registering them. Use the following procedure to de-register an authentication card.

1. Select the authentication card on the **Authentication Card** table.
2. Click **Deregister**.
3. A confirmation dialog box is displayed. Click **OK** to confirm de-registration.

   The **Encryption Group** dialog box displays.

4. Click **OK** on the **Encryption Group** dialog box.

   The card is de-registered from the group.

Using authentication cards

When a quorum of authentication cards are registered for use, an **Authenticate** dialog box is displayed to grant access to the following:

- The **Encryption Group Properties** dialog box **Security** tab.
- The **Encryption Group Properties** dialog box **Link Keys** tab.
- The **Master Key Backup** dialog box.
- The **Master Key Restore** dialog box.
- The **Edit System Card** dialog box.

To authenticate using a quorum of authentication cards, do the following:

1. When the **Authenticate** dialog box is displayed, gather the number of cards needed, as directed by instructions on the dialog box. The currently registered cards and the assigned owners are listed in the table near the bottom of the dialog box.
2. Insert a card, and wait for the ID to appear in the **Card ID** field.
3. Enter the assigned password.
4. Click **Authenticate**.
5. Wait for the confirmation dialog box, and click **OK**.
6. Repeat steps two through five for each card until the quorum is reached.
7. Click **OK**.

Registering system cards from a card reader

System cards are smart cards that can be used to control activation of encryption engines. Encryption switches and blades have a card reader that enables the use of a system card. System cards discourage theft of encryption switches or blades by requiring the use of a system card at the switch or blade to enable the encryption engine. When the switch or blade is powered off, the encryption engine will not work without first inserting a system card into its card reader. If someone removes a switch or blade with the intent of accessing the encryption engine, it will function as an ordinary FC switch or blade when it is powered up, but use of the encryption engine is denied.

To register a system card from a card reader, a smart card must physically available. System cards can be registered during encryption group or member configuration when running the configuration wizard, or they can be registered using the following procedure.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select the switch from the **Encryption Devices** table, and select **Switch > System Cards** from the menu task bar, or right-click the switch or and select **System Card**.

   The **Register System Card** dialog box is displayed.

3. Insert a smart card into the card reader. Be sure to wait for the card serial number to appear, and then enter card assignment information, as directed.

4. Click **OK**.

5. Wait for the confirmation dialog box indicating initialization is done, and click **OK**.

   The card is added to the **Registered System Cards** table on the **System Cards** dialog box.

6. Store the card in a secure location, not in the proximity of the switch or blade.

De-registering a system card

System cards can be removed from the database by de-registering them. Use the following procedure to de-register a system card.

1. From the **Register System Card** dialog box, select the system card you want to de-register.

2. Click **Deregister**.

3. A confirmation dialog box is displayed. Click **OK** to confirm de-registration.

   The card is removed to the **Registered System Cards** table.

Enabling or disabling the system card requirement

If you want to use a system card to control activation of an encryption engine on a switch, you must enable the system card requirement. You can use the following procedure to enable or disable the system card requirement.

1. From the **Encryption Center** select an encryption group, and select the **Security** menu.

   The **Select Security Settings** dialog is displayed.

2. Set **System Cards** to **Required** to require the use a system card to control activation of an encryption engine. If **System Cards** is set to **Not Required**, the encryption engine activates without the need to read a system card first.

3. Click **OK**.

Viewing and editing switch encryption properties

To view switch encryption properties, complete the following steps.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays the status of all encryption-related hardware and functions at a glance. It is the single launching point for all encryption-related configuration.

2. Select the switch or encryption engine from the **Encryption Devices** table, and select **Switch > Properties** or **Engine > Properties** from the menu bar, or right-click the switch or encryption engine and select **Properties**.

   The **Encryption Properties** dialog box, shown in Figure 106, contains the following information:

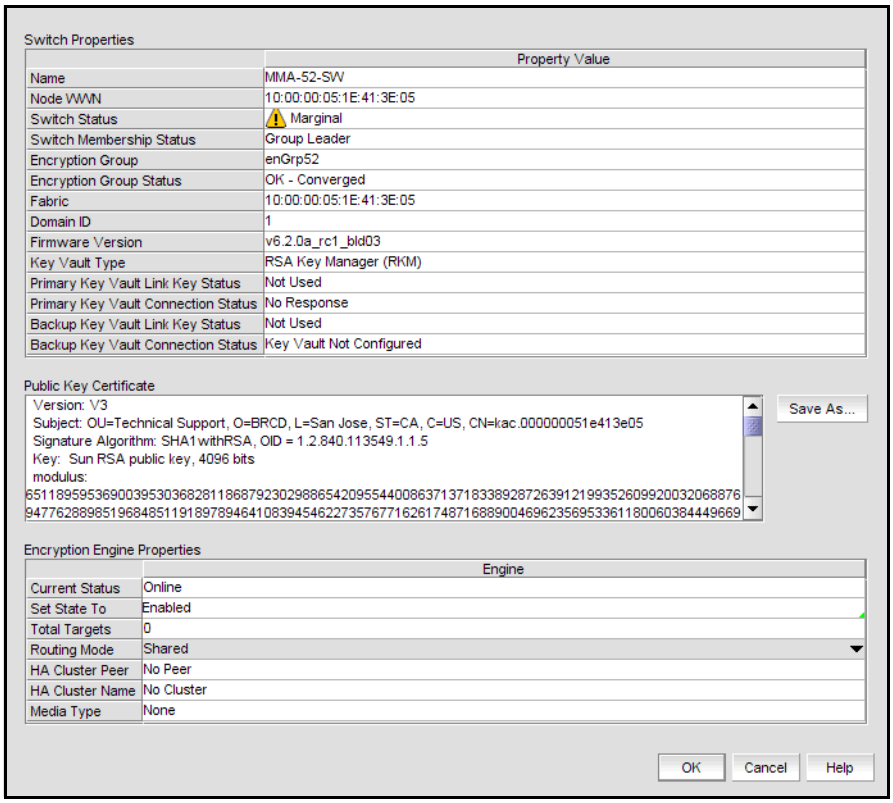


FIGURE 106 Encryption Properties dialog box

- **Switch Properties** table - the properties associated with the selected switch.
- **Name** - the name of the selected switch.
- **Node WWN** - the world wide name of the node.
- **Switch Status** - the health status of the switch. Possible values are Healthy, Marginal, Down, Unknown, Unmonitored, and Unreachable.
- **Switch Membership Status** - the alert or informational message description which details the health status of the switch. Possible values are Group Member, Leader-Member Comm, Error, Discovering, and Not a member.
- **Encryption Group** - the name of the encryption group to which the switch belongs.
- **Encryption Group Status** - Possible values are:
  - **OK - Converged** - the group leader can communicate with all members.
  - **Degraded** - the group leader cannot communicate with one or more members.
  - **Unknown** - the group leader is in an unmanaged fabric.

NOTE
When a group is in the **Degraded** state, the following operations are not allowed: key vault changes, master key operations, enable/disable encryption engines, Failback mode changes, HA Cluster creation or addition (removal is allowed), and any configuration changes for storage targets, hosts, and LUNs.

- **Fabric** - the name of the fabric to which the switch belongs.
- **Domain ID** - the domain ID of the selected switch.

- **Firmware Version** - the current encryption firmware on the switch.
- **Primary Key Vault Link Key Status** - the possible statuses are as follows:
  - **Not Used** – the key vault type is not LKM.
  - **No Link Key** – no access request was sent to an LKM yet, or a previous request was not accepted.
  - **Waiting for LKM approval** – a request was sent to LKM and is waiting for the LKM administrator's approval.
  - **Waiting for local approval** – a response was received from LKM.
  - **Created, not validated** – the interim state until first used.
  - **OK** – a shared link key exists and has been successfully used.
- **Primary Key Vault Connection Status** - whether the primary key vault link is connected. Possible values are Unknown, Key Vault Not Configured, No Response, Failed authentication, and Connected.
- **Backup Key Vault Link Key Status** - the possible statuses are as follows:
  - **Not Used** – the key vault type is not LKM.
  - **No Link Key** – no access request was sent to an LKM yet, or a previous request was not accepted.
  - **Waiting for LKM approval** – a request was sent to LKM and is waiting for the LKM administrator's approval.
  - **Waiting for local approval** – a response was received from LKM.
  - **Created, not validated** – the interim state until first used.
  - **OK** – a shared link key exists and has been successfully used.
- **Backup Key Vault Connection Status** - whether the backup key vault link is connected. Possible values are Unknown, Key Vault Not Configured, No Response, Failed authentication, and Connected.
- **Public Key Certificate** text box - the switch's KAC certificate, which must be installed on the primary and backup key vaults.
- **Save As** button - saves the certificate to a file in PEM format. The file may be loaded into the key vault using the key vault's tools.
- **Encryption Engine Properties** table - the properties for the encryption engine. There may be 0 to 4 slots, one for each encryption engine in the switch.
- **Current Status** - the status of the encryption engine. There are many possible values, but common values are Not Available (the engine is not initialized), Disabled, Operational, need master/link key, and Online.
- **Set State To** - enter a new value, enabled or disabled, and click OK to apply the change.
- **Total Targets** - the number of the encrypted target device.
- **Routing Mode** - the routing mode of the encryption engine. Only Shared is supported for this release.
- **HA Cluster Peer** - the name and location of the high-availability (HA) cluster peer (another encryption engine in the same group), if in an HA configuration.

- **HA Cluster Name** - the name of the HA cluster (for example, Cluster1), if in an HA configuration. The name can have a maximum of 31 characters. Only letters, digits, and underscores are allowed.
- **Media Type** - the media type of the encryption engine. Possible values are Disk and Tape.
- **System Card** - the current status of system card information for the encryption engine. (registered or not registered).

Saving the public key certificate

To save the certificate to a file in PEM format, complete the following steps.

1. Click **Save As**.

   The **Save** dialog box displays.

2. Browse to the location where you want to save the certificate.
3. Click **Save**.

   You can now load the file into the key vault using the key vault's tools.

Enabling the encryption engine state

To enable the encryption engine state, complete the following steps.

1. Select **Enabled** from the **Set State To** list.
2. Click **OK**.

Disabling the encryption engine state

To disable the encryption engine state, complete the following steps.

1. Select **Disabled** from the **Set State To** list.
2. Click **OK**.

Viewing and editing group properties

To view encryption group properties, complete the following steps.

1. Select **Configure > Encryption**.

   The **Encryption Center** dialog box displays.

2. If groups are not visible in the **Encryption Devices** table, select **View > Groups** from the menu bar.

   The encryption groups display in the **Encryption Devices** table.

3. Select a group from the **Encryption Devices** table, and select **Group > Properties** from the menu bar, or right-click the group and select **Properties**.

   The **Encryption Group Properties** dialog box, shown in Figure 106, has six tabs which are defined in this section:

   - "General tab" on page 325
   - "Members tab" on page 325
   - "Security tab" on page 328
   - "HA Clusters tab" on page 329
   - "Engine Operations tab" on page 329
   - "Link Keys tab" on page 330
   - "Tape Pools tab" on page 331

NOTE
The **Link Keys** tab appears only if the key vault type is NetApp LKM.

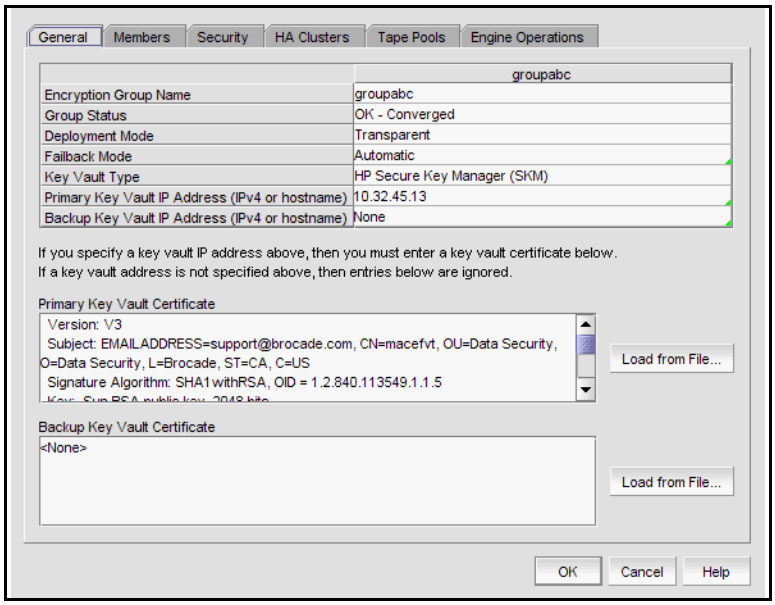


FIGURE 107 Encryption Group Properties dialog box

General tab

The properties displayed in the **General** tab are described below.

- **Encryption group name** - the name of the encryption group.
- **Group status** - the status of the encryption group, which can be **OK-Converged** or **Degraded**. Degraded means the group leader cannot contact all of the configured group members.
- **Deployment mode** - the group's deployment mode, which is transparent.
- **Failback mode** - The group's failback mode, which can be automatic or manual. For Fabric OS versions earlier than 6.2.0, the failback mode must be set manually using the CLI.
- **Key vault** - the vault type, either RSA Key Manager (RKM) NetApp Lifetime Key Manager (LKM), HP Secure Key Manager (SKM), or nCipher Key Authority (NCKA).
- **Primary key vault IP address** - The IP address of the primary key vault, either IPv4 or host name.
- **Backup key vault IP address** - the IP address of the backup key vault.
- **Primary key vault certificate** - the details of the primary vault certificate; for example, version and signature information.
- **Backup key vault certificate** - the details of the backup vault certificate; for example, version and signature information.

Members tab

The **Group Members** tab lists group switches, their role, and their connection status with the group leader. The tab displays the configured membership for the group (none of the table columns are editable). The list can be different from the members displayed in the **Encryption Center** dialog box if some configured members are unmanaged, missing, or in a different group.

Possible **Connection Status** values are as follows:

- **Group Leader** - this switch is the group leader so there is no connection status.
- **Trying to Contact** - the member is not responding to the group leader. This may occur if the member switch is not reachable by way of the management port, or if the member switch does not believe it is part of the encryption group.
- **Configuring** - the member switch has responded and the group leader is exchanging information. This is a transient condition that exists for a short time after a switch is added or restored to a group.
- **OK** - the member switch is responding to the group leader switch.
- **Not Available** - the group leader is not a managed switch, so connection statuses are not being collected from the group leader.

Members tab Remove button

You can click the **Remove** button to remove a selected switch or an encryption group from the encryption group table.

- You cannot remove the group leader unless it is the only switch in the group. If you remove the group leader, the Management application also removes the HA cluster, the target container, and the tape pool (if configured) that are associated with the switch.
- If you remove a switch from an encryption group, the Management application also removes the HA cluster and target container associated with the switch.

NOTE
If the encryption group is in a degraded state, the Management application does not remove the HA clusters or target containers associated with the switch. In this case, a pop-up error message displays.

- If you remove the last switch from a group, the Management application also deletes the group.

Consequences of removing an encryption switch

Table 33 explains the impact of removing switches.

TABLE 33 Switch removal warnings

Switch configuration	Impact of removal
The switch is the only switch in the encryption group.	The encryption group is also removed.
The switch has configured encryption targets on encryption engines.	• The switch is configured to encrypt traffic to one or more encryption targets. • The target container configuration is removed. • The encrypted data remains on the encryption target but is not usable until the encryption target is manually configured on another encryption switch. **CAUTION** **The encryption target data is visible in encrypted format to zoned hosts. It is strongly recommended that you remove the encryption targets from all zones before you disable encryption. Otherwise, hosts may corrupt the encrypted data by writing directly to the encryption target without encryption.**
The switch has encryption engines in HA Clusters.	The HA Clusters are removed. High availability is no longer provided to the other encryption engine in each HA Cluster.

Figure 108 shows the warning message that displays if you click **Remove** to remove a switch.

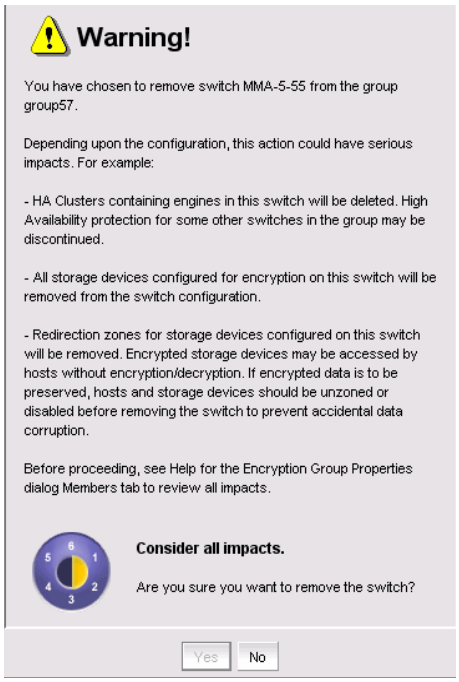

Warning!
You have chosen to remove switch MMA-5-55 from the group group57.
Depending upon the configuration, this action could have serious impacts. For example:
- HA Clusters containing engines in this switch will be deleted. High Availability protection for some other switches in the group may be discontinued.
- All storage devices configured for encryption on this switch will be removed from the switch configuration.
- Redirection zones for storage devices configured on this switch will be removed. Encrypted storage devices may be accessed by hosts without encryption/decryption. If encrypted data is to be preserved, hosts and storage devices should be unzoned or disabled before removing the switch to prevent accidental data corruption.
Before proceeding, see Help for the Encryption Group Properties dialog Members tab to review all impacts.
Consider all impacts.
Are you sure you want to remove the switch?
Yes
No

FIGURE 108 Removal of switch warning

Figure 109 shows the warning message that displays if you click **Remove** to remove an encryption group.

Warning!
Switch MMA-7-56-SW is the last switch in group DemoKV. Removing the switch will also delete the Encryption Group.
Depending upon the configuration, this action could have serious impacts. For example:
- All Tape Pools and HA Clusters configured for this Encryption Group will be removed.
- All storage devices configured for encryption will be removed from the switch configuration.
- Redirection zones for storage devices will be removed. Encrypted storage devices may be accessed by hosts without encryption/decryption. If encrypted data is to be preserved, hosts and storage devices should be unzoned or disabled before deleting the Encryption Group to prevent accidental data corruption.
Before proceeding, see Help for the Encryption Group Properties dialog Members tab to review all impacts.
Consider all impacts.
Are you sure you want to delete the Encryption Group?
Yes
No

FIGURE 109 Removal of switch in encryption group warning

Security tab

The **Security** tab (Figure 110) displays the status of the master key for the encryption group.

NOTE
You must enable encryption engines before you back up or restore master keys.

Master key actions are as follows:

- **Back up a master key**, which is enabled any time a master key exists.
- **Restore a master key**, which is enabled when either no master key exists or the previous master key has been backed up.
- **Create a new master key**, which is enabled when no master key exists or the previous master key has been backed up.

See "Master keys" on page 363 for complete information about managing master keys.

NOTE
Encryption is not allowed until the master key has been backed up.

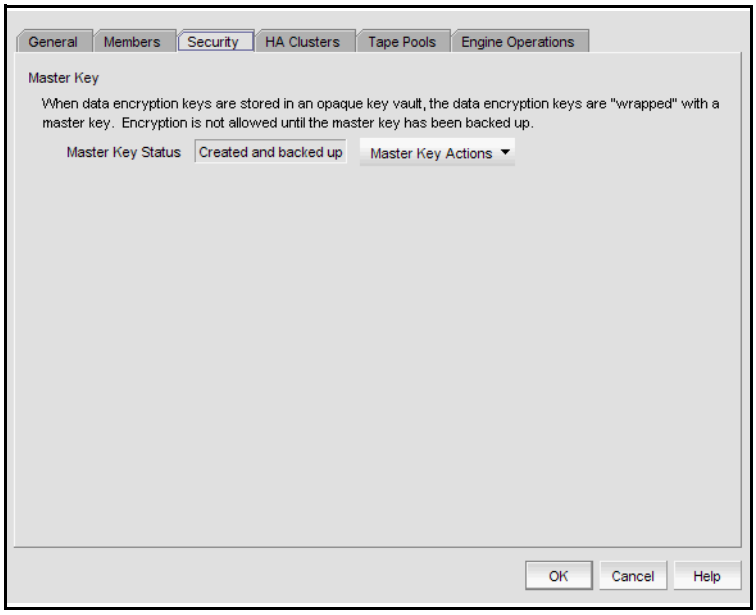

General
Members
Security
HA Clusters
Tape Pools
Engine Operations
Master Key
When data encryption keys are stored in an opaque key vault, the data encryption keys are "wrapped" with a master key. Encryption is not allowed until the master key has been backed up.
Master Key Status
Created and backed up
Master Key Actions
OK
Cancel
Help

FIGURE 110 Encryption Group Properties - Security tab

HA Clusters tab

HA clusters are groups of encryption engines that provide high availability features. If one of the engines in the group fails or becomes unreachable, the other cluster member takes over the encryption and decryption tasks of the failed encryption engine. An HA cluster consists of exactly two encryption engines. See "Creating high availability (HA) clusters" on page 347.

The **HA Clusters** tab (Figure 111) allows you to create and delete HA clusters, add encryption engines to and remove encryption engines from HA clusters, and failback an engine.

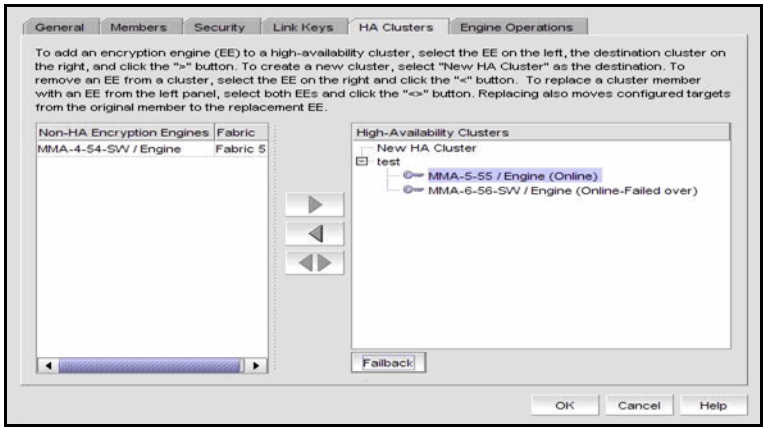

General
Members
Security
Link Keys
HA Clusters
Engine Operations
To add an encryption engine (EE) to a high-availability cluster, select the EE on the left, the destination cluster on the right, and click the ">" button. To create a new cluster, select "New HA Cluster" as the destination. To remove an EE from a cluster, select the EE on the right and click the "<" button. To replace a cluster member with an EE from the left panel, select both EEs and click the "<>" button. Replacing also moves configured targets from the original member to the replacement EE.
Non-HA Encryption Engines
Fabric
MMA-4-54-SW / Engine
Fabric 5
High-Availability Clusters
New HA Cluster
test
MMA-5-55 / Engine (Online)
MMA-6-56-SW / Engine (Online-Failed over)
Failback
OK
Cancel
Help

FIGURE 111 **Encryption Group Properties - HA Clusters tab**

Engine Operations tab

The **Engine Operations** tab (Figure 112) enables you to replace an encryption engine in an encryption switch with another encryption engine in another switch within a DEK Cluster environment. A DEK Cluster is a set of encryption engines that encrypt the same target storage device. DEK Clusters do not display in the Management application, they are an internal implementation feature and have no user-configurable properties.

NOTE

You cannot replace an encryption engine if it is part of an HA Cluster. For information about HA Clusters, refer to "HA Clusters tab" on page 329.

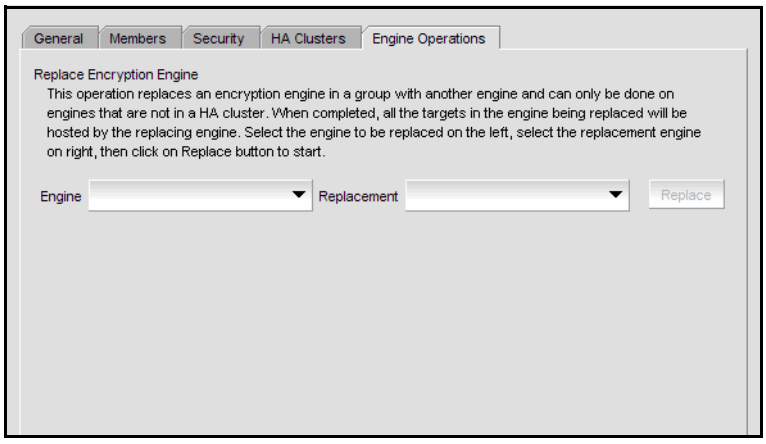

General
Members
Security
HA Clusters
Engine Operations
Replace Encryption Engine
This operation replaces an encryption engine in a group with another engine and can only be done on engines that are not in a HA cluster. When completed, all the targets in the engine being replaced will be hosted by the replacing engine. Select the engine to be replaced on the left, select the replacement engine on right, then click on Replace button to start.
Engine
Replacement
Replace

FIGURE 112 **Encryption Group Properties - HA Clusters tab**

Replacing an encryption engine

To replace an encryption engine in an encryption group with another encryption engine within a DEK Cluster, complete the following steps.

1. Select **Configure > Encryption**.

   The **Encryption Center** dialog box displays.

2. If groups are not visible in the **Encryption Devices** table, select **View > Groups** from the menu bar.

   The encryption groups display in the **Encryption Devices** table.

3. Select an encryption group from the tree, and select **Group > Properties** from the menu bar, or right-click the encryption group and select **Properties**.

   The **Encryption Group Properties** dialog box displays.

4. Click the **Engine Operations** tab.
5. Select the engine you want to replace in the **Engine** list.
6. Select the engine you want to use as the replacement in the **Replacement** list.
7. Click **Replace**.

   All containers hosted by the current engine (**Engine** list) are replaced by the new engine (**Replacement** list).

Link Keys tab

Connections between a switch and an NetApp LKM key vault require a shared link key. Link keys are used only with LKM key vaults. They are used to protect data encryption keys in transit to and from the key vault. There is a separate link key for each key vault for each switch. The link keys are configured for a switch but are stored in the encryption engines, and all the encryption engines in a group share the same link keys.

You must create link keys under the following circumstances:

- When a new encryption group is created.
- When a new switch is added to an encryption group.
- When a new key vault is added to an encryption group.
- After all encryption engines in a switch have been zeroized.
- When all of the encryption blades have been removed from a director and one or more new encryption blades have been added.

The **Link Keys** tab displays a table that shows link key status for each switch in an encryption group.

Tape Pools tab

Tape pools are managed from the **Tape Pools** tab.

Figure 113 displays the tape pools tab.

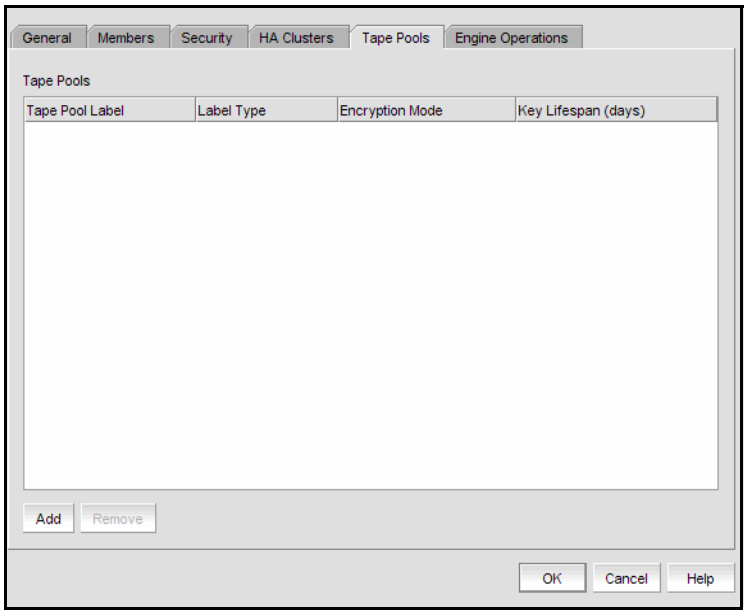


FIGURE 113 Encryption Group Properties - Tape Pools tab

- If you want to remove a tape pool, select one or more tape pools in the list and click **Remove**.
- To modify the tape pool, remove the entry and add a new tape pool. See "Adding tape pools" on page 332 for more information.

Tape pools overview

Tape cartridges and volumes may be organized into a tape pool (a collection of tape media). The same data encryption keys are used for all cartridges and volumes in the pool. Tape pools are used by backup application programs to group all the tape volumes used in a single backup or in a backup plan. The tape pool name or number used must be the same name or number used by the host backup application. If the same tape pool name or number is configured for an encryption group, tapes in that tape pool are encrypted according to the tape pool settings instead of the tape LUN settings.

Encryption switches and encryption blades support tape encryption at the tape pool level (for most backup applications) and at the LUN (tape drive) level. Since Tape Pool policies override the LUN (tape drive) policies, the LUN pool policies are used only if no tape pools exist, or if the tape media/volume does not belong to any configured tape pools.

All encryption engines in the encryption group share the tape pool definitions. Tapes can be encrypted by an encryption engine, where the container for the tape target LUN is hosted. The tape media is mounted on the tape target LUN.

Tape pool definitions are not needed to read a tape. Tape pool definitions are only used when writing to tape.

Adding tape pools

A tape pool can be identified by either a name or a number, but not both. Tape pool names and numbers must be unique within the encryption group. When a new encryption group is created, any existing tape pools in the switch are removed and must be added.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. If groups are not visible in the **Encryption Devices** table, select **View > Groups** from the menu bar.

   The encryption groups display in the **Encryption Devices** table.

3. Select an encryption group from the tree, and select **Group > Tape Pools** from the menu bar, or right-click the encryption group and select **Tapepools**.

   The **Add Tape Pool** dialog box displays. The **Name** tape pool label type is the default; however, you can change the tape pool label type to its number by selecting **Number**, shown in Figure 115.

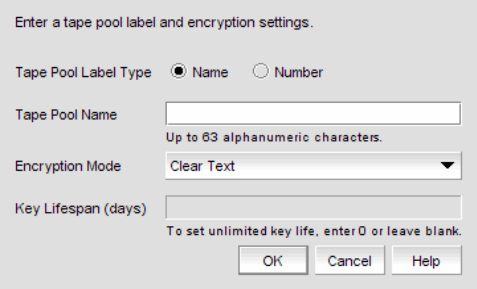


FIGURE 114 Add Tape Pool by name dialog box

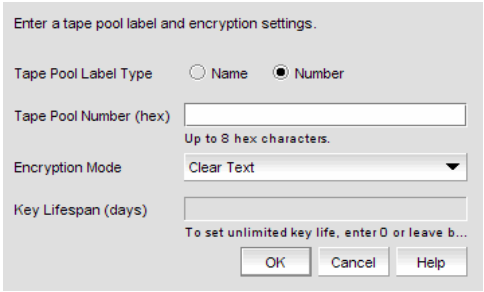


FIGURE 115 Add Tape Pool by number dialog box

4. Specify the **Tape Pool Label Type**. Tape pools can be identified by either a name or a number, shown in Figure 114 and Figure 115.

5. Enter a name for the tape pool. If you selected **Number** as the **Tape Pool Label Type**, the name must match the tape pool label or tape ID/number that is configured on the tape backup/restore application.

6. Select the **Encryption Mode**.

   Choices include **Clear Text**, **DF-Compatible Encryption**, and **Native Encryption**. **DF-Compatible Encryption** is valid only when LKM is the key vault. The **Key Lifespan (days)** field is editable only if the tape pool is encrypted. If **Clear Text** is selected as the encryption mode, the key lifespan is disabled.

   NOTE
   You cannot change the encryption mode after the tape pool I/O begins.

7. Enter the number of days that you want to use a key before obtaining a new key, if you want to enforce a key lifespan. The default is Infinite (a blank field or a value of `0`).

   NOTE
   The key lifespan interval represents the key expiry timeout period for tapes or tape pools. You can only enter the **Key Lifespan** field if the tape pool is encrypted. If **Clear Text** is selected as the encryption mode, the **Key Lifespan** field is disabled.

8. Click **OK**.

Encryption Targets dialog box

The **Encryption Targets** dialog box enables you to send outbound data that you want to store as ciphertext to an encryption device. The encryption target acts as a virtual target when receiving data from a host, and as a virtual initiator when writing the encrypted data to storage.

To access the Encryption Targets dialog box, complete the following steps.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays, showing the status of all encryption-related hardware and functions.

2. Select the **Group >Targets**, **Switch > Targets**, or **Engine > Targets,** from the tool bar menu, or right-click on the group, switch, or encryption engine in the **Encryption Devices** table, and select **Targets**.

   The **Encryption Targets** dialog box (Figure 116) displays the targets currently being encrypted by the selected group, switch, or encryption engine. If a group is selected, all configured targets in the group are displayed. If a switch is selected, all configured targets for the switch are displayed.

   The **Encryption Targets** dialog box enables you to launch a variety of wizards and other related dialog boxes, which are defined in Table 34.

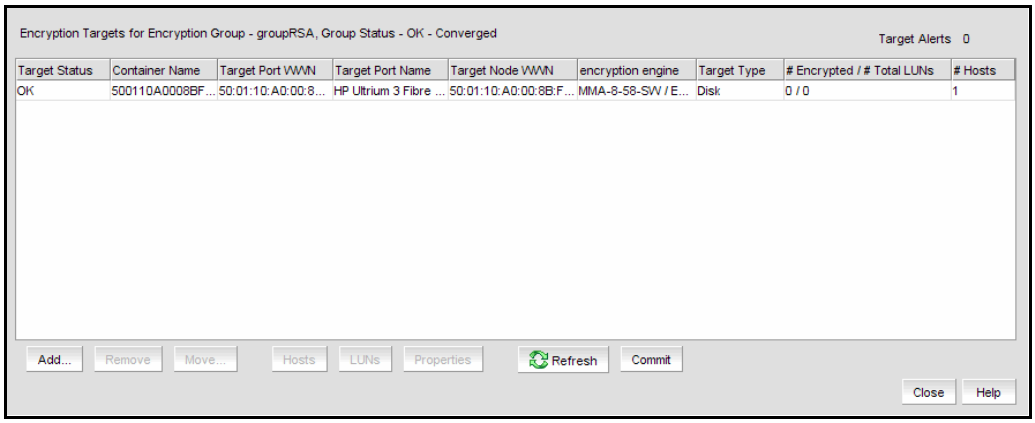


FIGURE 116 Encryption Targets dialog box

TABLE 34 Encryption Targets dialog box functionality

Feature	Description
Add button	Launches the **Storage Encryption Setup Wizard**, which enables you to configure a new target for encryption. It is the first step in configuring encryption for a storage device. It is recommended that you zone the host and target together before you add container information. • **Note:** If the group is in **OK-Converged** mode, the group leader can communicate with all members. The **Configure Storage Encryption** wizard dialog box launches when you click **Add**. **Note**: • If a group is in the **Degraded** state, the following operations are not allowed: key vault changes, master key operations, enable/disable encryption engines, failback mode changes, HA Cluster creation or addition (removal is allowed), tape pool changes, and any configuration changes for storage targets, hosts, and LUNs. • If a group is in the **Unknown** state, the group leader is in an unmanaged fabric.
Remove button	Removes a selected target. Proceed only if the data on the LUN is to be disabled or if the LUN is to be configured for encryption again on some other encryption engine. If the LUN data is to be enabled and later accessed by way of another encryption engine, you should unzone the host with the encryption engine *before* you remove the encryption target from the encryption engine. This prevents the host from accidentally writing to the encryption target during the unencrypted interim period. **CAUTION** **Removing a selected target can result in data loss, if the host is writing to the target as it is removed. Removing the target will result in lost access to the data, but the data remains encrypted on the target.**
Move button	Moves one encryption target to a different encryption engine. The target and engine must be in the same encryption group.

TABLE 34 Encryption Targets dialog box functionality (Continued)

Feature	Description
Hosts button	Launches the **Encryption Target Hosts** dialog box, where you can configure hosts to access the selected encryption target.
LUNs button	Launches the **Encryption Target LUNs** dialog box, where you can display existing LUNs and add new LUNs. The button is enabled only if there are hosts associated with the targets.
Commit button	Commits LUN changes, including adding, removing, or modifying disk or tape LUNs. If there are multiple paths to the same physical LUNs, then the LUNs are added to multiple target containers (one target per storage device port). When adding, modifying, or removing multi-pathed LUNs, make the same changes in all target containers, and then click Commit to apply all the changes at once. This keeps the LUN settings consistent on each path. There is a limit of 25 LUN changes, including adding, modifying, or removing LUNs, per Commit operation. **Note:** The **Commit** button can also be used to re-create any redirection zones that were accidentally modified or removed.
Abort button	Aborts all transactions that have been configured but are not yet committed.
Properties button	Launches the **Encryption Target Properties** dialog box.
Refresh button	Refreshes the displayed data from the database maintained on the server. It does not collect new information from the hardware switches.

Redirection zones

It is recommended that you zone the host and target together before configuring them for encryption. Configuring a host/target pair for encryption normally creates a re-direction zone to redirect the host-target traffic through the encryption engine. But redirection zones can only be created if the host and target are already zoned. If the host and target are not already zoned, you can still configure them for encryption, but afterward you will need to zone the host and target together, and then click the **Commit** button to create the re-direction zones as a separate step.

NOTE
If you click the **Commit** button and the encryption group is busy, you are given the option to force the commit or abort the changes. Click the **Commit** button to re-create the redirection zones.

Creating a new encryption group

The following steps describe how to start and run the encryption setup wizard, and then create a new encryption group.

NOTE
When a new encryption group is created, any existing tape pools in the switch are removed.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

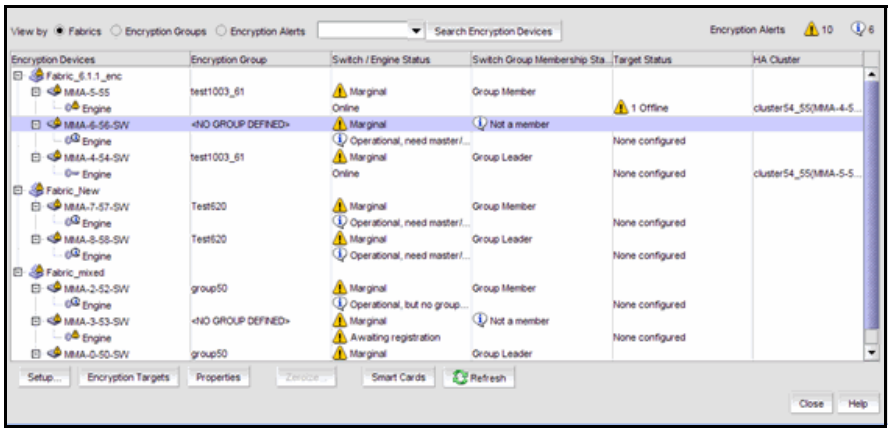


FIGURE 117 Encryption Center - No Group Defined dialog box

2. Select a switch from the **<NO GROUP DEFINED>** encryption group. The switch must not be in an encryption group already.
3. Select **Switch > Create/Add to Group**, or right-click the switch and select **Create/Add to Group.**

   The **Configure Switch Encryption** welcome panel displays.

4. Click **Next**.

   Create a new encryption Group is pre-selected. This is the correct selection for creating a new group.

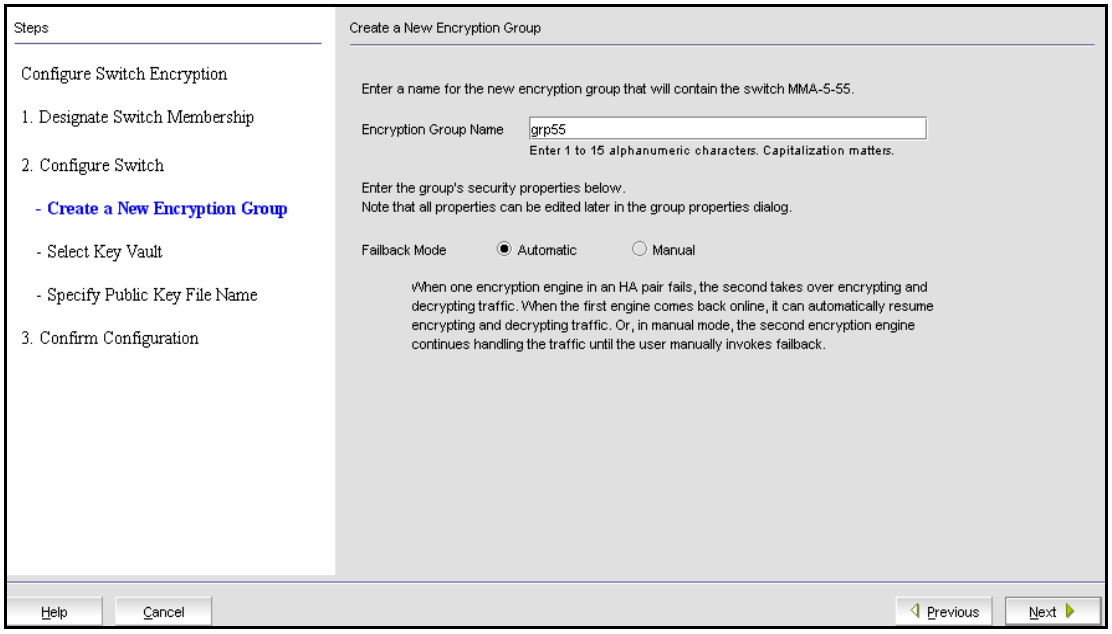

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Public Key File Name
3. Confirm Configuration
Create a New Encryption Group
Enter a name for the new encryption group that will contain the switch MMA-5-55.
Encryption Group Name
grp55
Enter 1 to 15 alphanumeric characters. Capitalization matters.
Enter the group's security properties below.
Note that all properties can be edited later in the group properties dialog.
Failback Mode
Automatic
Manual
When one encryption engine in an HA pair fails, the second takes over encrypting and decrypting traffic. When the first engine comes back online, it can automatically resume encrypting and decrypting traffic. Or, in manual mode, the second encryption engine continues handling the traffic until the user manually invokes failback.
Help
Cancel
Previous
Next

FIGURE 118 **Designate Switch Membership dialog box**

5. Click **Next**.

   The **Create a New Encryption Group** dialog box displays.

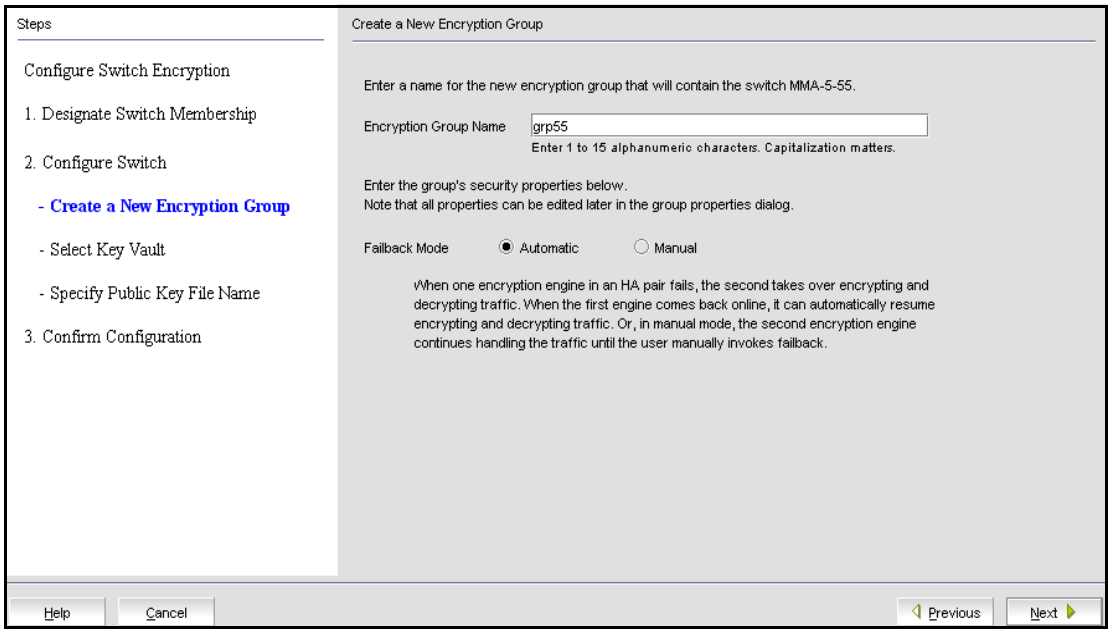

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Public Key File Name
3. Confirm Configuration
Create a New Encryption Group
Enter a name for the new encryption group that will contain the switch MMA-5-55.
Encryption Group Name
grp55
Enter 1 to 15 alphanumeric characters. Capitalization matters.
Enter the group's security properties below.
Note that all properties can be edited later in the group properties dialog.
Failback Mode
Automatic
Manual
When one encryption engine in an HA pair fails, the second takes over encrypting and decrypting traffic. When the first engine comes back online, it can automatically resume encrypting and decrypting traffic. Or, in manual mode, the second encryption engine continues handling the traffic until the user manually invokes failback.
Help
Cancel
Previous
Next

FIGURE 119 **Create a new encryption group dialog box**

6. Enter an **Encryption Group Name** for the encryption group (the maximum length of the group name is 15 characters; letters, digits, and underscores are allowed) and select the **Automatic** failback mode.

NOTE
If the name you enter for the encryption group already exists, a pop-up warning message displays. Although unique group names avoid confusion while managing multiple groups, you are not prevented from using duplicate group names. Click **Yes** to use the same name for the new encryption group, or click **No** to enter a new, unique name.

7. Click **Next**.

   The **Select Key Vault** dialog box displays.

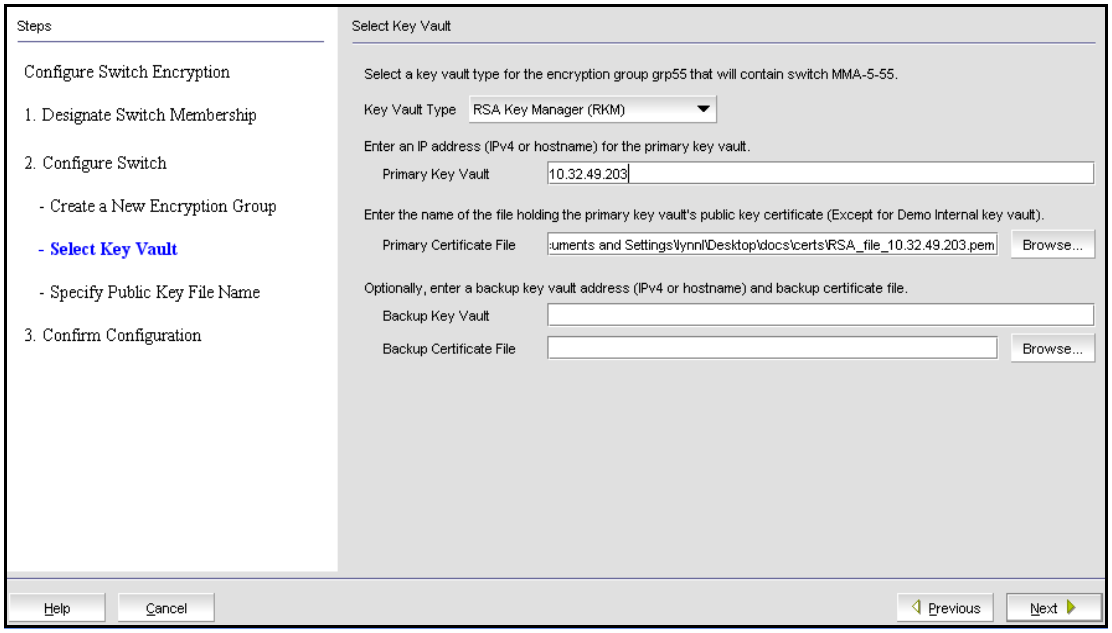

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Public Key File Name
3. Confirm Configuration
Select Key Vault
Select a key vault type for the encryption group grp55 that will contain switch MMA-5-55.
Key Vault Type
RSA Key Manager (RKM)
Enter an IP address (IPv4 or hostname) for the primary key vault.
Primary Key Vault
10.32.49.203
Enter the name of the file holding the primary key vault's public key certificate (Except for Demo Internal key vault).
Primary Certificate File
:uments and Settings\lynnl\Desktop\docs\certs\RSA_file_10.32.49.203.pem
Browse...
Optionally, enter a backup key vault address (IPv4 or hostname) and backup certificate file.
Backup Key Vault
Backup Certificate File
Browse...
Help
Cancel
Previous
Next

FIGURE 120 Select Key Vault dialog box

8. Select the **Key Vault Type**. The choices are the following:
   - RKM - RSA Key Manager
   - LKM - NetApp Link Key Manager
   - SKM - HP Secure Key Manager
   - NCKA - Thales Encryption Manager for Storage (TEMS)
9. Enter the IP address or host name for the primary key vault.

   When a new key vault IP address or host name is entered, you must also enter the name of the file that holds the primary key vault's public key certificate (or browse to the location by clicking the **Browse** button).
10. Enter the name of the file holding the primary key vault's public key certificate.

    If you are using a backup key vault, also enter the IP address or host name, and the name of the file holding the backup key vault's public key certificate in the fields provided.

Key vault address changes

Before you add or change a key vault address, you must install the public key certificates for all switches in the encryption group on the key vault. Use the **Encryption Group Properties** dialog box to check a switch's connection status to the new key vault and to obtain the switch's public key certificate.

If you remove a primary key vault IP address, and a backup key vault has been configured, you can use the backup, but no new disk LUNs can be encrypted, no disk LUNs can be re-keyed, and no new tape LUNs can be encrypted. New tapes in a tape pool that has an existing DEK can be encrypted. Existing disk and tape LUNs can still be decrypted.

11. Click **Next**.

    The **Specify Public Key Certificate Filename** panel displays.

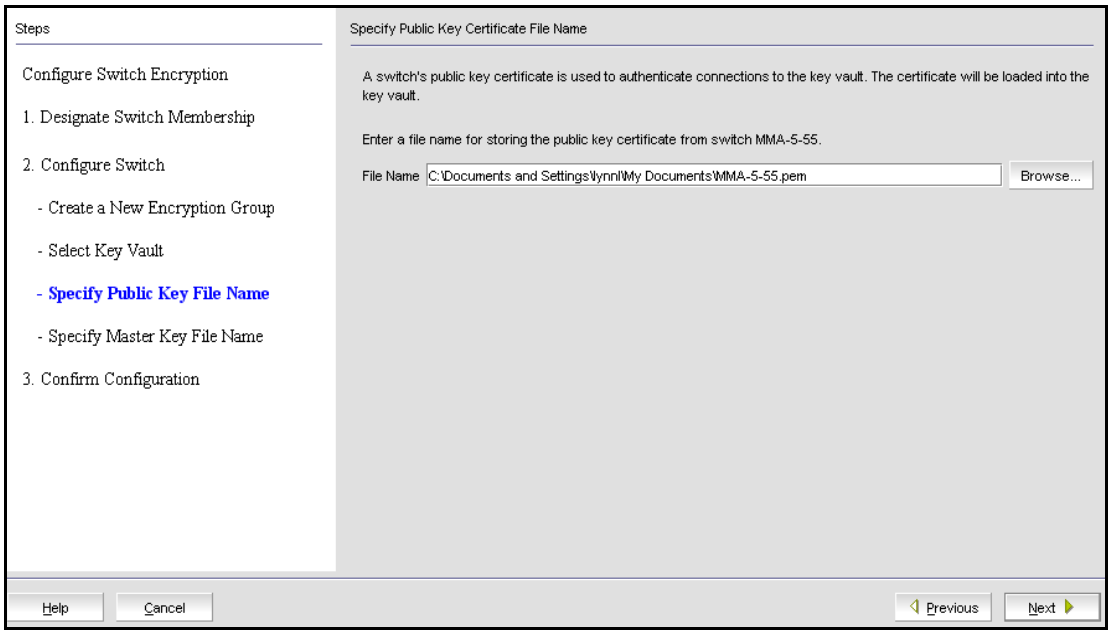

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Public Key File Name
- Specify Master Key File Name
3. Confirm Configuration
Specify Public Key Certificate File Name
A switch's public key certificate is used to authenticate connections to the key vault. The certificate will be loaded into the key vault.
Enter a file name for storing the public key certificate from switch MMA-5-55.
File Name
C:\Documents and Settings\lynn\My Documents\MMA-5-55.pem
Browse...
Help
Cancel
Previous
Next

FIGURE 121 Specify Public Key Certificate filename dialog box

12. Specify the name of the file where you want to store the public key certificate that is used to authenticate connections to the key vault, and click **Next**.

    The certificate stored in this file is the switch's public key certificate. You will need to know this path and file name to install the switch's public key certificate on the key management appliance.

13. Click **Next**.

    If you chose LKM as the **Key Vault Type**, the **Confirm Configuration** panel displays (skip to step 18).

    For all other supported key vault types, the **Specify Master Key File Name** panel displays.

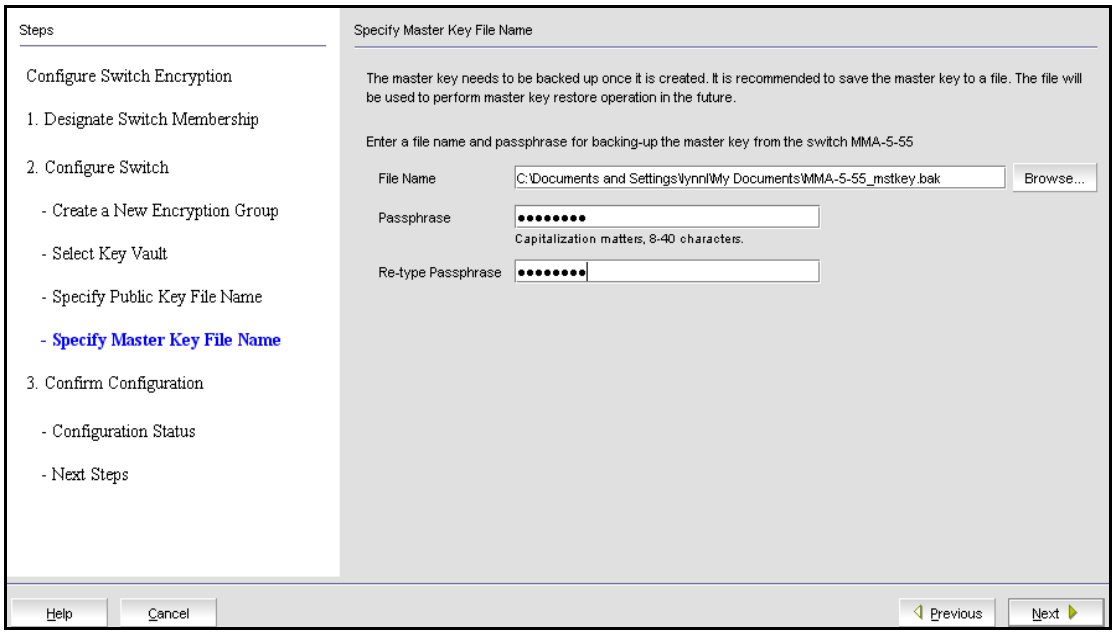

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Public Key File Name
- Specify Master Key File Name
3. Confirm Configuration
- Configuration Status
- Next Steps
Specify Master Key File Name
The master key needs to be backed up once it is created. It is recommended to save the master key to a file. The file will be used to perform master key restore operation in the future.
Enter a file name and passphrase for backing-up the master key from the switch MMA-5-55
File Name
C:\Documents and Settings\lynnl\My Documents\MMA-5-55_mstkey.bak
Browse...
Passphrase
Capitalization matters, 8-40 characters.
Re-type Passphrase
Help
Cancel
Previous
Next

FIGURE 122 Specify Master Key File Name dialog box

14. Enter a file name, or browse to the desired location.
15. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.
16. Re-type the passphrase for verification.

17. Click **Next**.

    The **Confirm Configuration** panel displays the encryption group name and switch public key certificate file name you specified, shown in Figure 123.

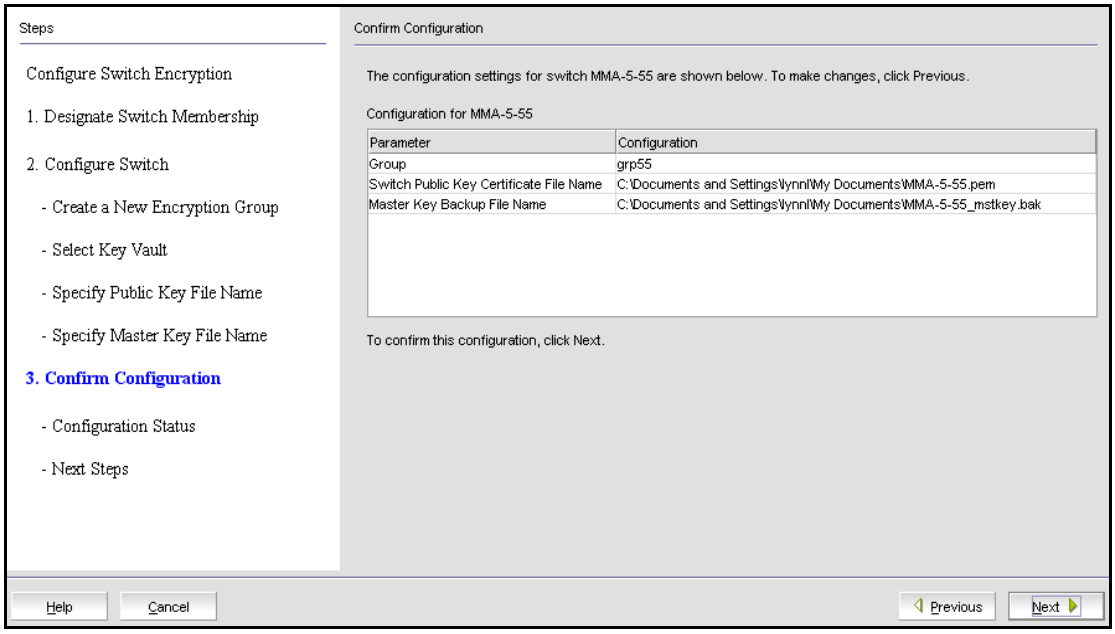


FIGURE 123 Confirm Configuration dialog box

18. Click **Next** to confirm the displayed information.

    The **Configuration Status** displays, as shown in Figure 124. The configuration status steps vary slightly depending on the key vault type.

    - A progress indicator shows that a configuration step is in progress. A green check mark indicates successful completion of all steps for that **Configuration Item**. A red stop sign indicates a failed step.
    - All **Configuration Item**s have green check marks if the configuration is successful. A message displays below the table, indicating that the encryption switch was added to the group you named, and the public key certificate is stored in the location you specified.

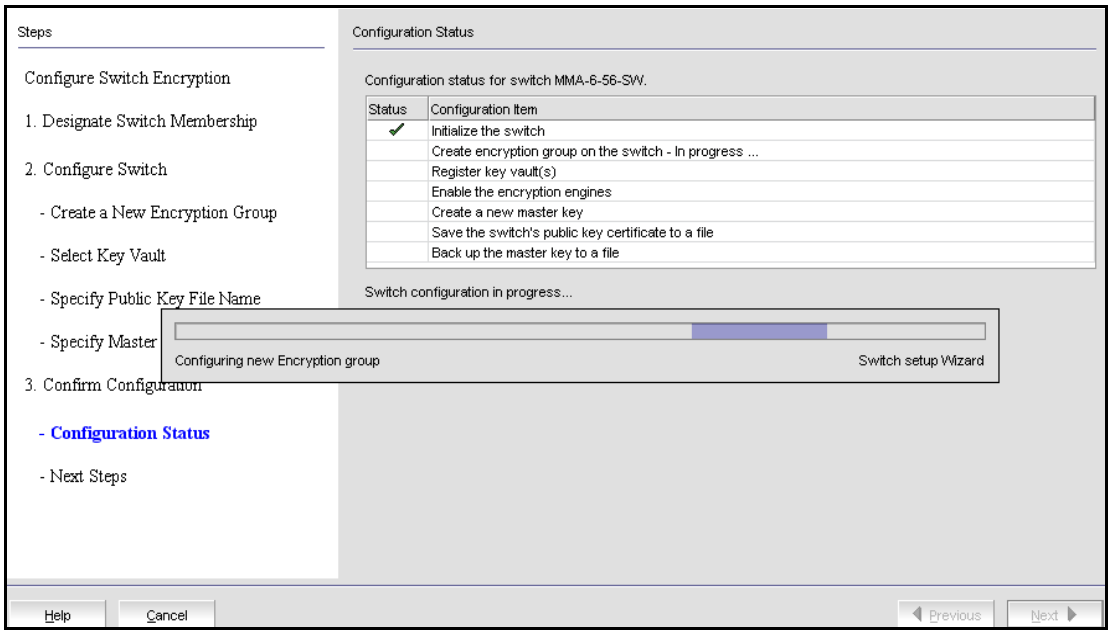


FIGURE 124 Configuration Status dialog box

The Management application sends API commands to verify the switch configuration. The CLI commands are detailed in the *Fabric OS Encryption Administrator's Guide, "Key vault configuration*."

- **Initialize the switch**

  If the switch is not already in the initiated state, the Management application performs the `cryptocfg --initnode` command.

- **Create encryption group on the switch**

  The Management application creates a new group using the `cryptocfg --create -encgroup` command, and sets the key vault type using the `cryptocfg --set -keyvault command`.

- **Register key vault(s)**

  The Management application registers the key vault using the `cryptocfg --reg keyvault` command.

- **Enable the encryption engines**

  The Management application initializes an encryption switch using the `cryptocfg --initEE [<slotnumber>]` and `cryptocfg --regEE [<slotnumber>]` commands.

- **Create a new master key**

  The Management application checks for a new master key. New master keys are generated from the Encryption Group Properties dialog box, Security tab. See "Creating a new master key" on page 372 for more information.

- **Save the switch's public key certificate to a file**

  The Management application saves the KAC certificate into the specified file.

- **Back up the master key to a file**

  The Management application saves the master key into the specified file. Note that a master key is not generated if the key vault type is LKM. LKM manages DEK exchanges through a trusted link, and the LKM appliance uses its own master key to encrypt DEKs.

19. Click **Next**.

    The **Read Instructions** dialog box displays instructions for installing public key certificates for the encryption switch. These instructions are specific to the key vault type. Copy or print these instructions.

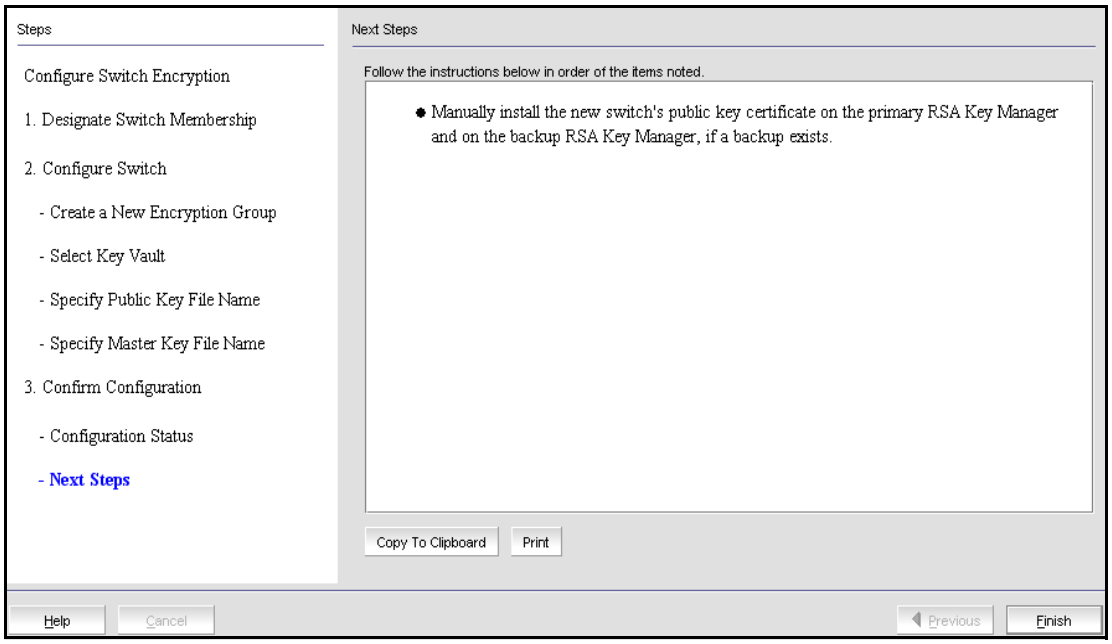

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Public Key File Name
- Specify Master Key File Name
3. Confirm Configuration
- Configuration Status
- Next Steps
Next Steps
Follow the instructions below in order of the items noted.
Manually install the new switch's public key certificate on the primary RSA Key Manager and on the backup RSA Key Manager, if a backup exists.
Copy To Clipboard
Print
Help
Cancel
Previous
Finish

FIGURE 125 **Read Instructions dialog box**

20. Click **Finish** to exit the **Configure Switch Encryption** wizard.

    At this point, a **Next Steps** dialog box is displayed, with brief instructions that are specific to certificate exchanges between the switch and key manager you are using. Refer to Appendix A, "Supported Key Management Systems" for more detailed instructions for certificate exchange with each supported key manager, and refer to the key manager user documentation for additional information.

Adding a switch to an encryption group

The setup wizard allows you to either create a new encryption group, or add an encryption switch to an existing encryption group. Use the following procedure to add a switch to an encryption group.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select the switch to be to be added to the group. The switch must not already be in an encryption group.

3. Select **Switch > Create/Add to Group**, or right-click the switch and select **Create/Add to Group.**

   The **Configure Switch Encryption** welcome panel displays.

4. Click **Next**.

   The **Designate Switch Membership** panel displays.

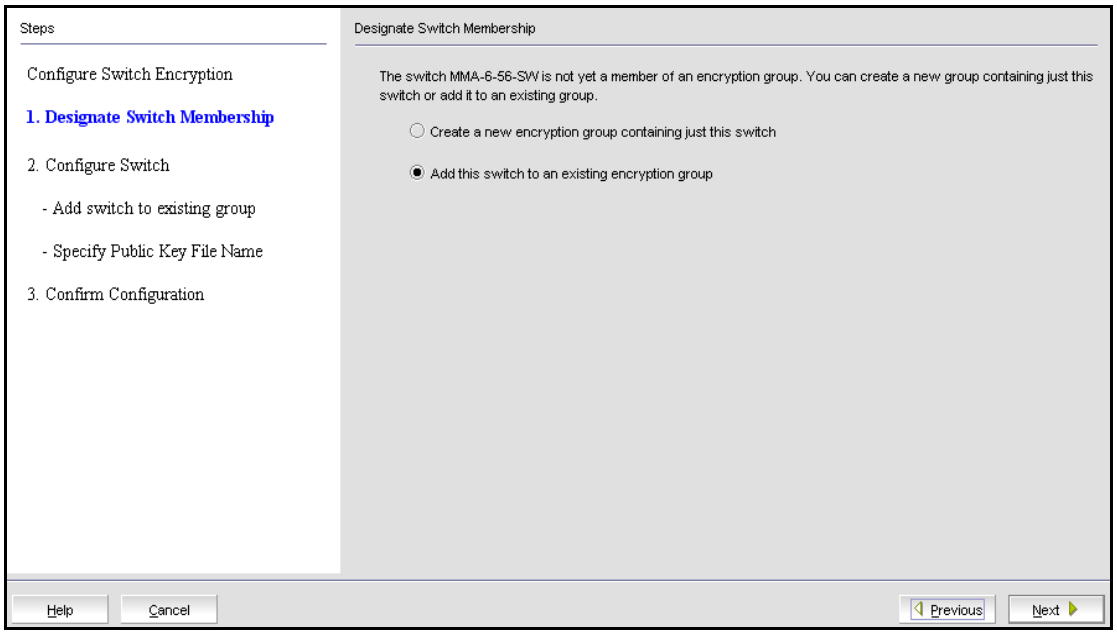

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Add switch to existing group
- Specify Public Key File Name
3. Confirm Configuration
Designate Switch Membership
The switch MMA-6-56-SW is not yet a member of an encryption group. You can create a new group containing just this switch or add it to an existing group.
Create a new encryption group containing just this switch
Add this switch to an existing encryption group
Help
Cancel
Previous
Next

FIGURE 126 **Add switch to an encryption group - Designate Switch Membership dialog box**

   a. Select **Add this switch to an existing encryption group**.

   b. Click **Next**.

   The **Add Switch to Existing Encryption Group** dialog box displays.

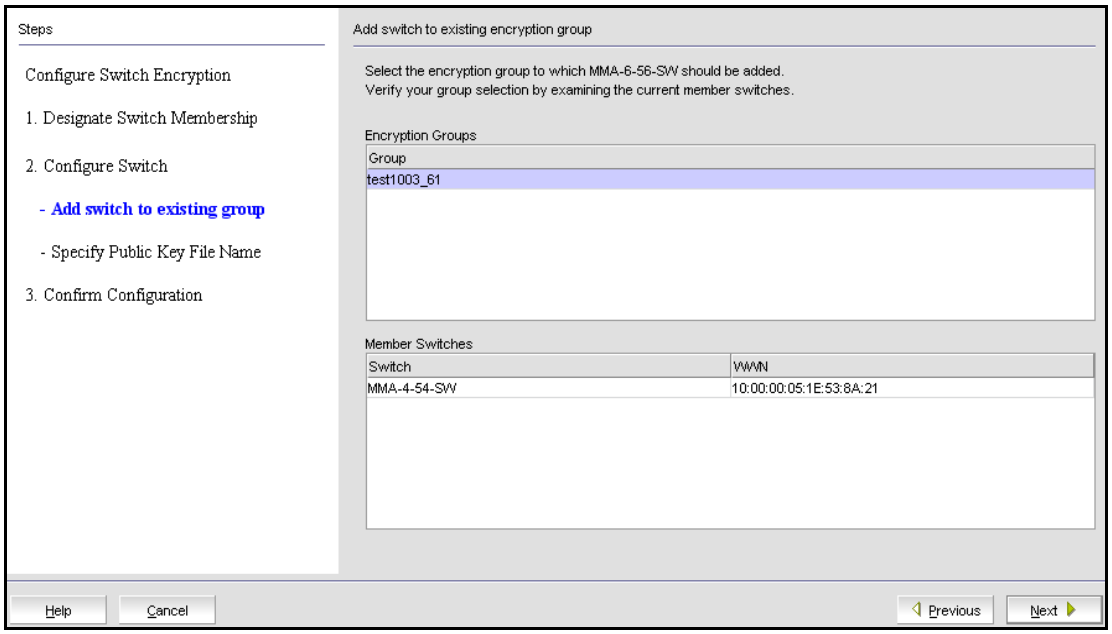


FIGURE 127 **Add Switch to Existing Encryption Group dialog box**

5. Select the group to which you want to add the switch, and click **Next**.

   The **Specify Public Key Certificate Filename** panel displays.

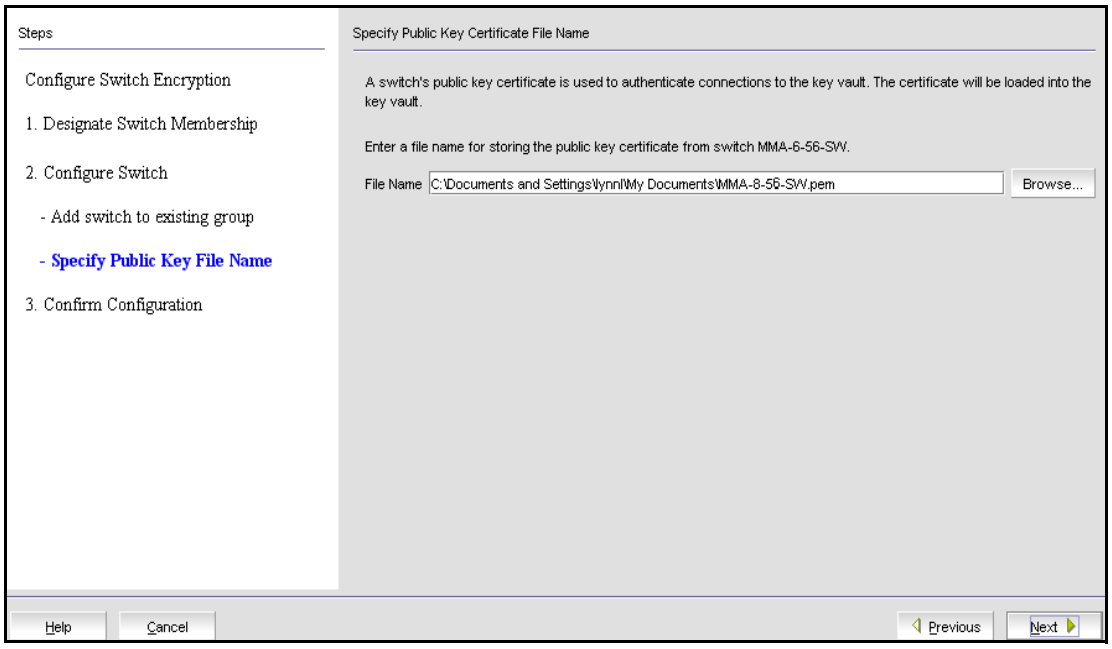

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Add switch to existing group
- Specify Public Key File Name
3. Confirm Configuration
Specify Public Key Certificate File Name
A switch's public key certificate is used to authenticate connections to the key vault. The certificate will be loaded into the key vault.
Enter a file name for storing the public key certificate from switch MMA-6-56-SW.
File Name
C:\Documents and Settings\lynnl\My Documents\MMA-8-56-SW.pem
Browse...
Help
Cancel
Previous
Next

FIGURE 128 **Add switch to an encryption group - Specify Public Key Certificate filename dialog box**

6. Specify the name of the file where you want to store the public key certificate that is used to authenticate connections to the key vault, and click **Next**.

   The **Confirm Configuration** panel displays the encryption group name and switch public key certificate file name you specified.

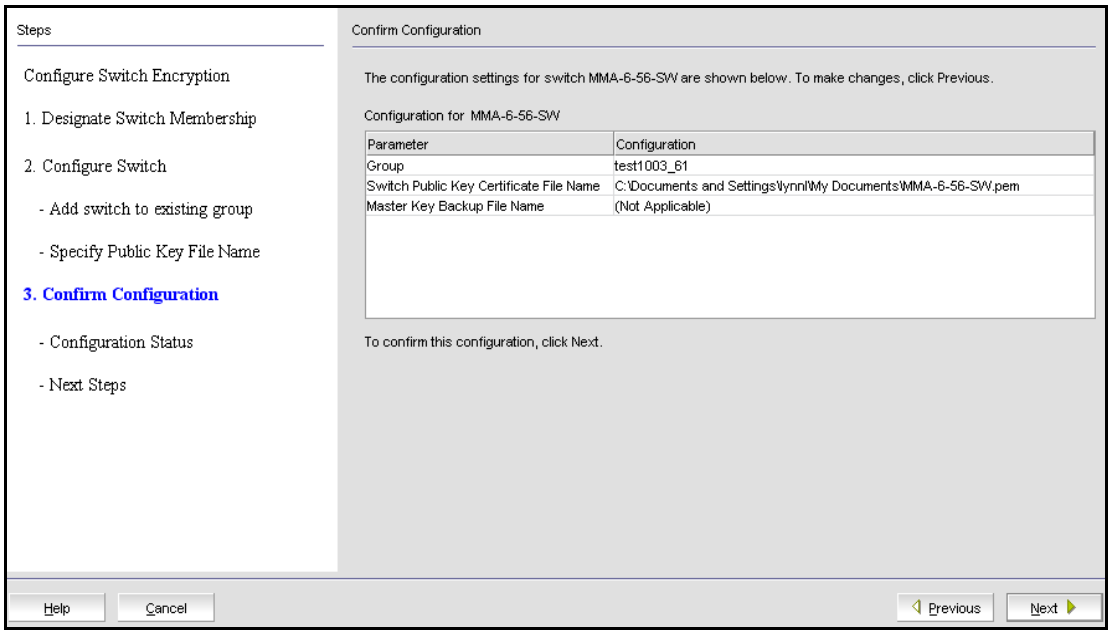


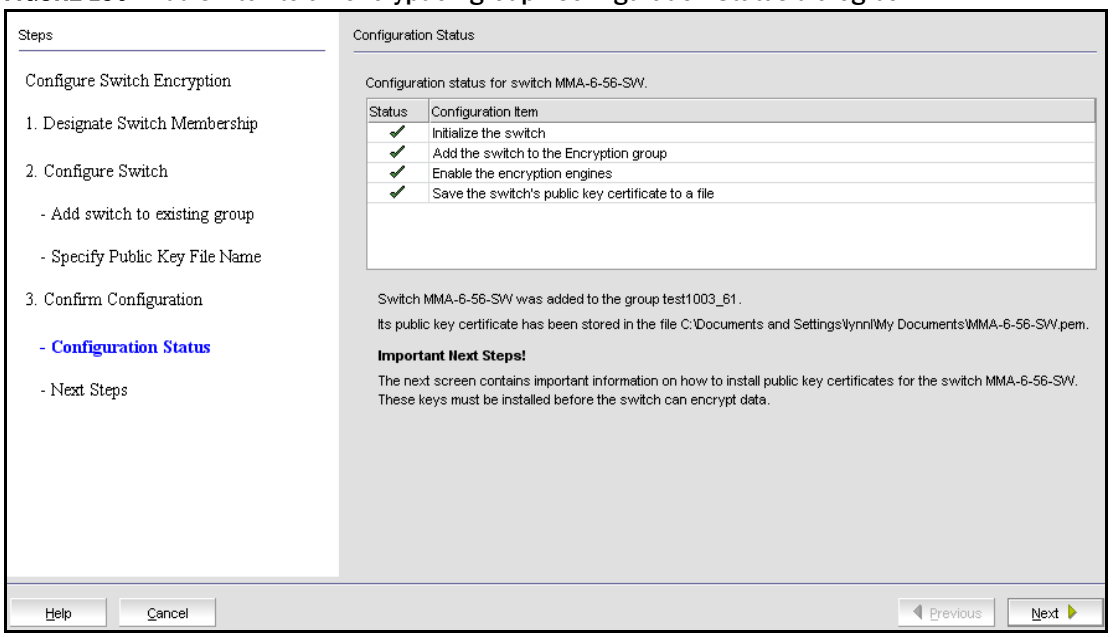
FIGURE 129 Add switch to an encryption group - Confirm Configuration dialog box

7. Click **Next** to confirm the displayed information.

   The **Configuration Status** displays.

   - A progress indicator shows that a configuration step is in progress. A green check mark indicates successful completion of all steps for that **Configuration Item**. A red stop sign indicates a failed step.
   - All **Configuration Item**s have green check marks if the configuration is successful. A message displays below the table, indicating that the encryption switch was added to the group you named, and the public key certificate is stored in the location you specified.

FIGURE 130 Add switch to an encryption group - Configuration Status dialog box


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Add switch to existing group
- Specify Public Key File Name
3. Confirm Configuration
- Configuration Status
- Next Steps
Configuration Status
Configuration status for switch MMA-6-56-SW.
Status
Configuration Item
Initialize the switch
Add the switch to the Encryption group
Enable the encryption engines
Save the switch's public key certificate to a file
Switch MMA-6-56-SW was added to the group test1003_61.
Its public key certificate has been stored in the file C:\Documents and Settings\lynnl\My Documents\MMA-6-56-SW.pem.
Important Next Steps!
The next screen contains important information on how to install public key certificates for the switch MMA-6-56-SW.
These keys must be installed before the switch can encrypt data.
Help
Cancel
Previous
Next

8. Note **Important Next Steps!** below this message, and click **Next**.

   Instructions for installing public key certificates for the encryption switch are displayed. These instructions are specific to the key vault type. Copy or print these instructions.

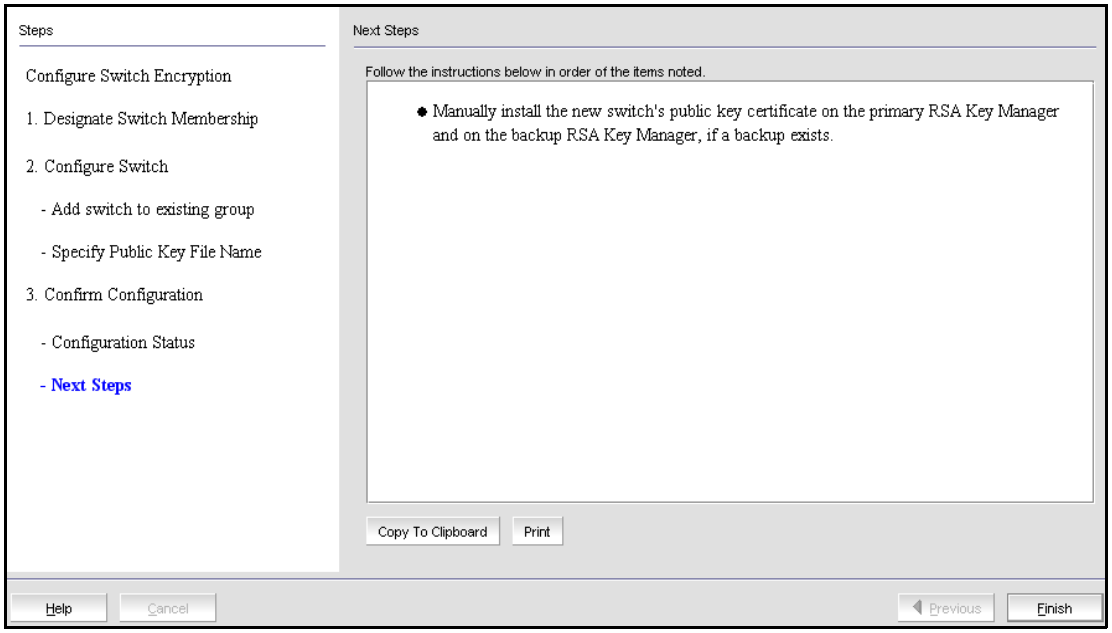

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Add switch to existing group
- Specify Public Key File Name
3. Confirm Configuration
- Configuration Status
- Next Steps
Next Steps
Follow the instructions below in order of the items noted.
Manually install the new switch's public key certificate on the primary RSA Key Manager and on the backup RSA Key Manager, if a backup exists.
Copy To Clipboard
Print
Help
Cancel
Previous
Finish

FIGURE 131 **Add switch to an encryption group - Next Steps dialog box**

9. Click **Finish** to exit the **Configure Switch Encryption** wizard.

Creating high availability (HA) clusters

A high availability (HA) cluster is a group of exactly two encryption engines. One encryption engine can take over encryption and decryption tasks for the other encryption engine, if that member fails or becomes unreachable.

When creating a new HA Cluster, add one engine to create the cluster and then add the second engine. You can make multiple changes to the HA Clusters list; the changes are not applied to the switch until you click **OK**.

Both engines in an HA cluster must be in the same fabric as well as the same encryption group.

NOTE
An IP address is required for the management port for any cluster-related operations.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. If groups are not visible in the **Encryption Devices** table, select **View > Groups** from the menu bar.

   The encryption groups display in the **Encryption Devices** table.

3. Select an encryption group from the tree, and select **Group > HA Cluster** from the menu bar, or right-click the encryption group and select **HA Cluster**.

   Encryption Group Properties are displayed, with the **HA Clusters** tab selected (Figure 132). Available encryption engines are listed under **Non-HA Encryption Engines**.

4. Select an available encryption engine, and a destination HA cluster under **High-Availability Clusters.** Select **New HA Cluster** if you are creating a new cluster.

5. Click the right arrow to add the encryption engine to the selected HA cluster.

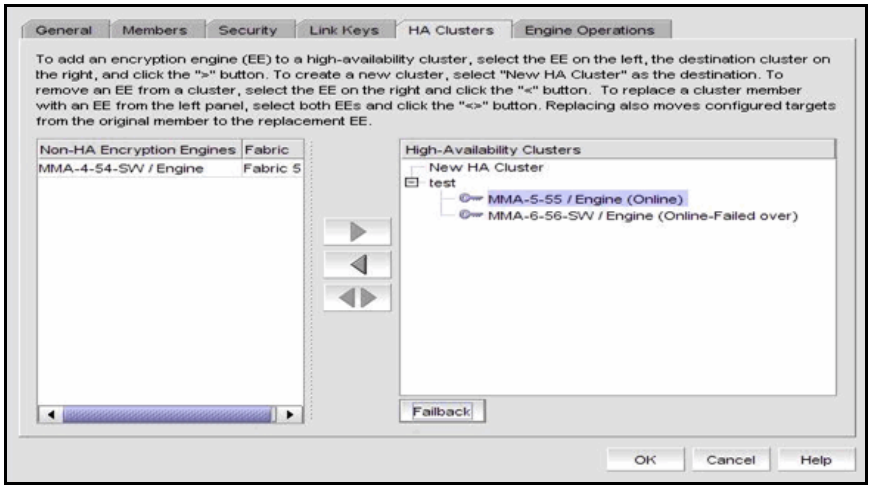

General
Members
Security
Link Keys
HA Clusters
Engine Operations
To add an encryption engine (EE) to a high-availability cluster, select the EE on the left, the destination cluster on the right, and click the ">" button. To create a new cluster, select "New HA Cluster" as the destination. To remove an EE from a cluster, select the EE on the right and click the "<" button. To replace a cluster member with an EE from the left panel, select both EEs and click the "<>" button. Replacing also moves configured targets from the original member to the replacement EE.
Non-HA Encryption Engines
Fabric
MMA-4-54-SW / Engine
Fabric 5
High-Availability Clusters
New HA Cluster
test
MMA-5-55 / Engine (Online)
MMA-6-56-SW / Engine (Online-Failed over)
Failback
OK
Cancel
Help

FIGURE 132 HA Clusters tab

NOTE
If you are creating a new HA cluster, a dialog box displays requesting a name for the new HA cluster. HA Cluster names can have up to 31 characters. Letters, digits, and underscores are allowed.

Removing engines from an HA cluster

Removing the last engine from an HA cluster also removes the HA cluster.

If only one engine is removed from a two-engine cluster, you must either add another engine to the cluster or the other engine must be removed too.

1. Select an encryption engine from the right tree (see Figure 132) and click the left arrow button.
2. Either remove the second engine or add a replacement second engine, making sure all HA clusters have exactly two engines.
3. Click **OK**.

Swapping engines in an HA cluster

Swapping engines is useful when replacing hardware. Swapping engines is different from removing an engine and adding another because when you swap engines, the configured targets on the former HA cluster member are moved to the new HA cluster member.

To swap engines, select one engine from the right tree (see Figure 132) and one unclustered engine from the list on the left, and click the double-arrow button.

NOTE
The two engines being swapped must be in the same fabric.

Failback option

The **Failback** option determines the behavior when a failed encryption engine is restarted. When the first encryption engine comes back online, the encryption group's failback setting (auto or manual) determines how the encryption engine resumes encrypting and decrypting traffic to its encryption targets.

- In auto mode, when the first encryption engine restarts, it automatically resumes encrypting and decrypting traffic to its encryption targets.
- In manual mode, the second encryption engine continues handling the traffic until you manually invoke failback using the CLI or Management application, or until the second encryption engine fails.

Invoking failback

To invoke failback to the restarted encryption engine from the Management application, complete the following steps.

1. Select **Configure > Encryption**.

   The **Encryption Center** dialog box displays.

2. Select the group to which the encryption engine belongs from the **Encryption Devices** table, and click **Properties**.

   The **Encryption Group Properties** dialog box displays.

3. Click the **HA Clusters** tab.
4. Select the online encryption engine and click **Failback**.
5. Click **OK** on the **Encryption Group Properties** dialog box.
6. Click **Close** on the **Encryption Center** dialog box.

Adding encryption targets

Adding an encryption target maps storage devices and hosts to virtual targets and virtual initiators within the encryption switch.

NOTE
It is recommended that you zone the host and target together before configuring them for encryption. If the host and target are not already zoned, you can still configure them for encryption, but afterward you will need to zone the host and target together, and then click the **Commit** button to commit the changes. If you attempt to close the Encryption Targets dialog box without committing the changes, you are reminded of uncommitted changes in the Management application.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays the status of all encryption-related hardware and functions at a glance. It is the single launching point for all encryption-related configuration

2. Select the encryption group, switch, or encryption engine to which you want to add the target.
3. Click **Encryption Targets**.

   The **Encryption Targets** dialog box displays.

4. Click **Add**.

   The **Configure Storage Encryption** welcome panel displays. The welcome panel explains the wizard's purpose, which is to configure encryption for a storage device (target).

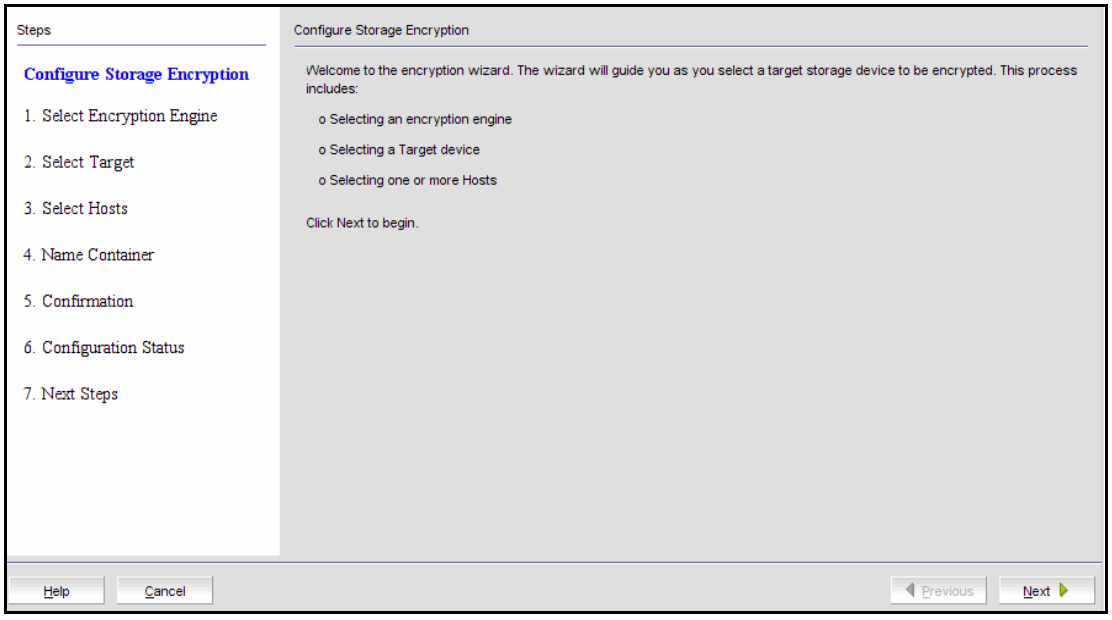


FIGURE 133 Configure Storage Encryption welcome panel

5. Click **Next** to begin.

   The **Select Encryption Engine** dialog box displays. The list of engines depends on the scope being viewed.

   - If the Targets dialog box is showing all targets in an encryption group, the list includes all engines in the group.
   - If the Targets dialog box is showing all targets for a switch, the list includes all encryption engines for the switch.
   - If the Targets dialog box is showing targets for a single encryption engine, the list contains only that engine.

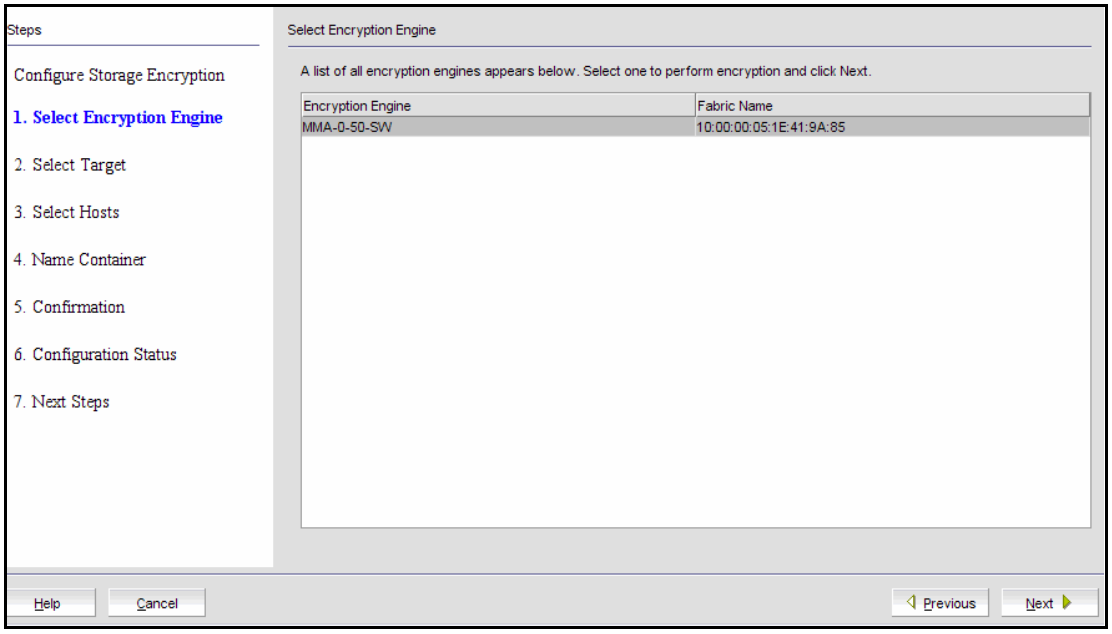


FIGURE 134 Select Encryption Engine dialog box

6. Select the encryption engine (blade or switch) you want to configure, and click **Next.**

   The **Select Target** panel displays. This panel lists all target ports and target nodes in the same fabric as the encryption engine. The **Select Target** list does *not* show targets that are already configured in an encryption group.

   There are two available methods for selecting targets: select from the list of known targets or manually enter the port and node WWNs.

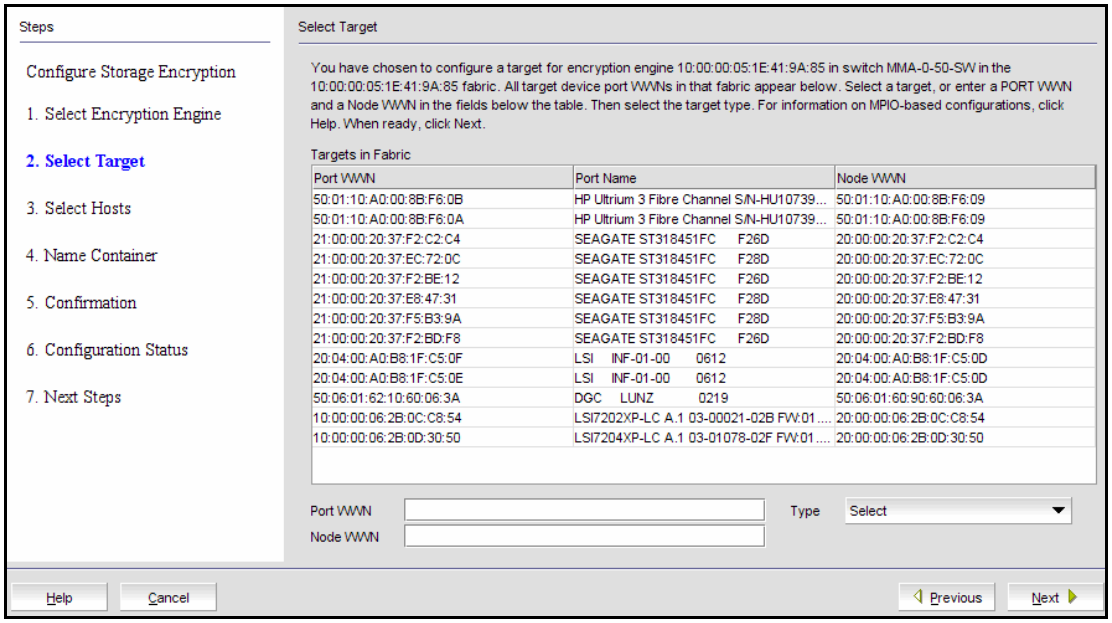

Steps
Configure Storage Encryption
1. Select Encryption Engine
2. Select Target
3. Select Hosts
4. Name Container
5. Confirmation
6. Configuration Status
7. Next Steps
Select Target
You have chosen to configure a target for encryption engine 10:00:00:05:1E:41:9A:85 in switch MMA-0-50-SW in the 10:00:00:05:1E:41:9A:85 fabric. All target device port WWNs in that fabric appear below. Select a target, or enter a PORT WWN and a Node WWN in the fields below the table. Then select the target type. For information on MPIO-based configurations, click Help. When ready, click Next.
Targets in Fabric
Port WWN
Port Name
Node WWN
50:01:10:A0:00:8B:F6:0B HP Ultrium 3 Fibre Channel S/N-HU10739... 50:01:10:A0:00:8B:F6:09
50:01:10:A0:00:8B:F6:0A HP Ultrium 3 Fibre Channel S/N-HU10739... 50:01:10:A0:00:8B:F6:09
21:00:00:20:37:F2:C2:C4 SEAGATE ST318451FC F26D 20:00:00:20:37:F2:C2:C4
21:00:00:20:37:EC:72:0C SEAGATE ST318451FC F28D 20:00:00:20:37:EC:72:0C
21:00:00:20:37:F2:BE:12 SEAGATE ST318451FC F26D 20:00:00:20:37:F2:BE:12
21:00:00:20:37:E8:47:31 SEAGATE ST318451FC F28D 20:00:00:20:37:E8:47:31
21:00:00:20:37:F5:B3:9A SEAGATE ST318451FC F28D 20:00:00:20:37:F5:B3:9A
21:00:00:20:37:F2:BD:F8 SEAGATE ST318451FC F26D 20:00:00:20:37:F2:BD:F8
20:04:00:A0:B8:1F:C5:0F LSI INF-01-00 0612 20:04:00:A0:B8:1F:C5:0D
20:04:00:A0:B8:1F:C5:0E LSI INF-01-00 0612 20:04:00:A0:B8:1F:C5:0D
50:06:01:62:10:60:06:3A DGC LUNZ 0219 50:06:01:60:90:60:06:3A
10:00:00:06:2B:0C:C8:54 LSI7202XP-LC A.1 03-00021-02B FW:01.... 20:00:00:06:2B:0C:C8:54
10:00:00:06:2B:0D:30:50 LSI7204XP-LC A.1 03-01078-02F FW:01.... 20:00:00:06:2B:0D:30:50
Port WWN
Node WWN
Type
Select
Help
Cancel
Previous
Next

FIGURE 135 Select Target dialog box

   a. Select a target from the list. (The **Target Port WWN** and **Target Node WWN** fields contain all the target information that displays using the `nsshow` command.) You can also enter WWNs manually if you prefer, or if you want to specify a target that is not on the list.

   b. Select a **Target Type**. Disk is selected and cannot be changed. If the target node is disk storage, choose **Disk**. If the target port is tape storage, choose **Tape**.

7. Click **Next**.

   The **Select Hosts** panel displays. This panel lists all hosts in the same fabric as the encryption engine. There are two available methods for selecting hosts: select from a list of known hosts or manually enter the port and node world wide names.

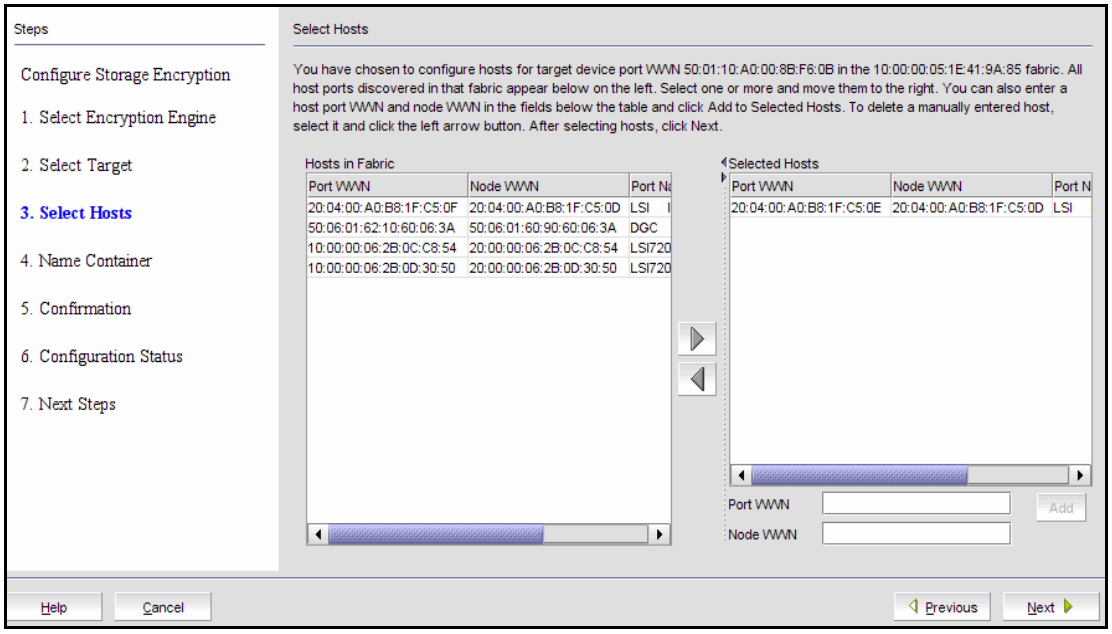


FIGURE 136 **Select Hosts dialog box**

   a. Select a maximum of 1024 hosts from the **Host Ports in Fabric** list, and click the right arrow to move the host to the **Selected Hosts** list. (The **Host Port WWN** column contains all the target information that displays using the `nsshow` command.)

   b. Manually enter world wide names in the **Host Port WWN** and **Host Port WWN** text boxes, if the hosts are not included in the list. You must fill in both the Host Port WWN and the Host Node WWN. Click the **Add to Selected Hosts** button to move the host to the **Selected Hosts** list.

8. Click **Next** when you are finished selecting hosts or manually entering the WWNs.

   The **Name Container** panel displays.

   The name container step in the wizard enables you to specify a name for the target container that is created in the encryption engine to hold the target configuration data.

9. The container name defaults to the target WWPN. You can, however, rename the container name. If you want to specify a name other than the default, enter a name, using a maximum number of 31 characters. Letters, digits, and underscores are allowed.

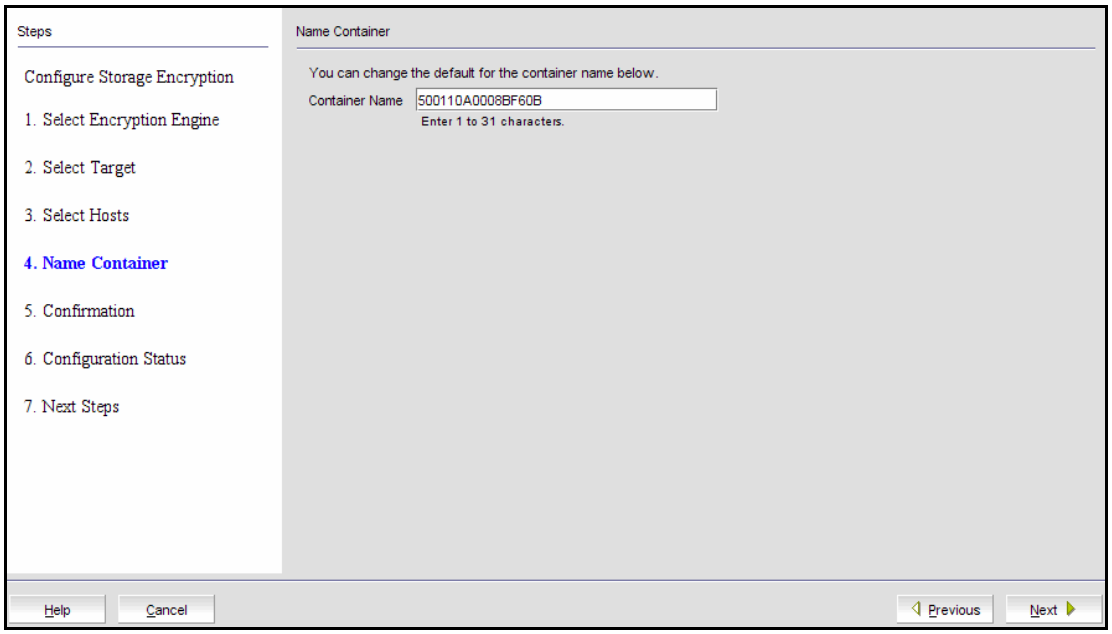


FIGURE 137 Name Container dialog box

10. Click **Next**.

    The **Confirmation** panel displays.

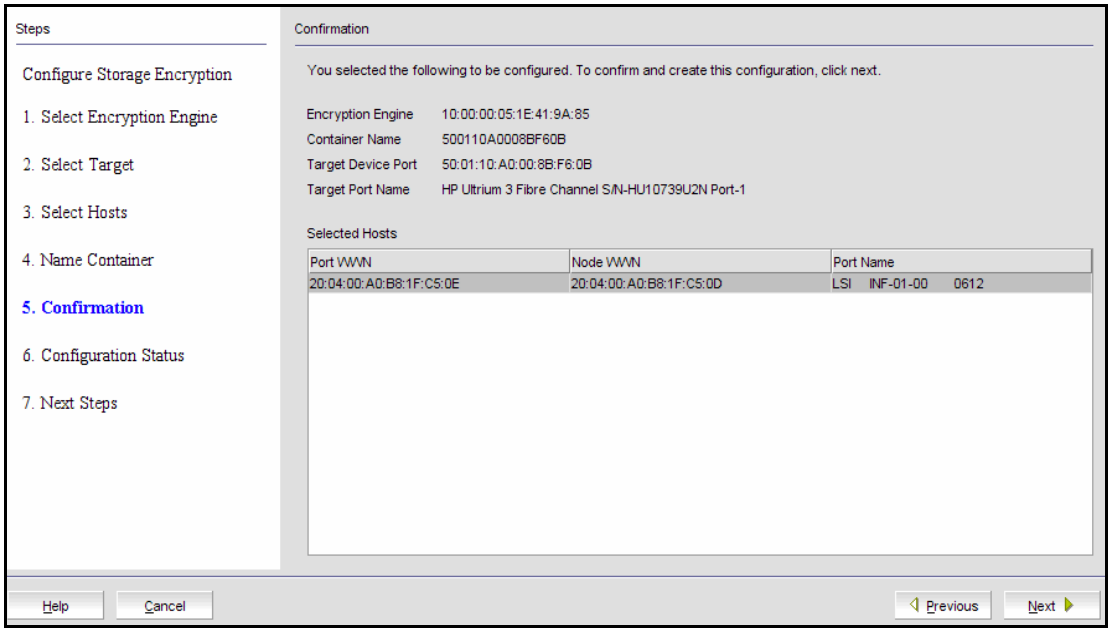


FIGURE 138 Confirmation dialog box

11. Click **Next** to confirm the displayed information.

    The **Configuration Status** displays the target and host that are configured in the target container, as well as the virtual targets (VT) and virtual initiators (VI).

NOTE
If you can view the VI/VT Port WWNs and VI/VT Node WWNs, the container has been successfully added to the switch.

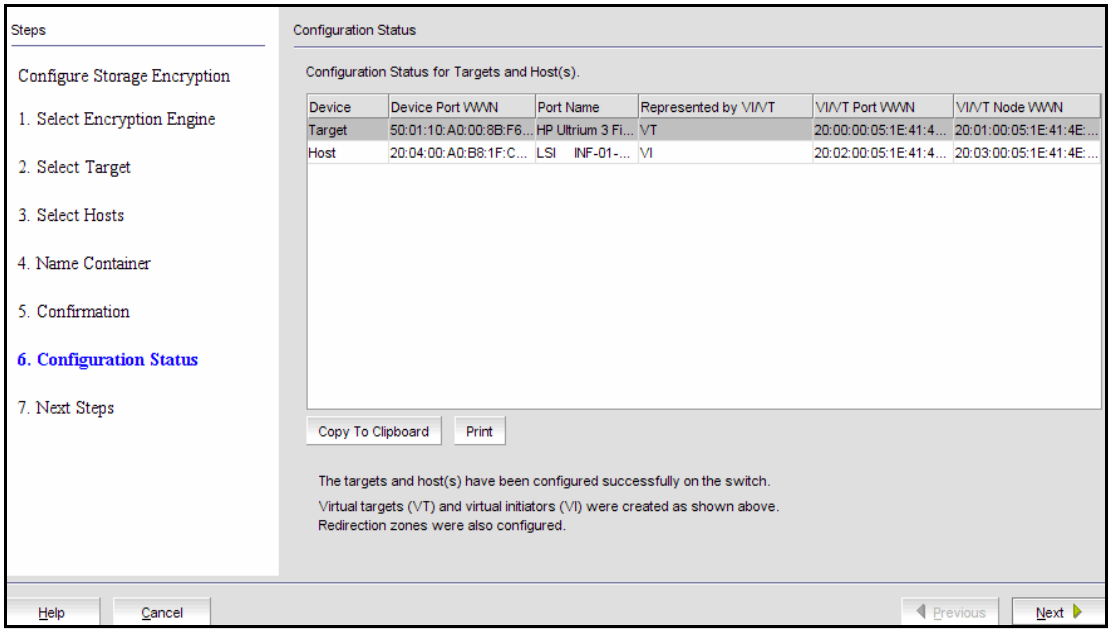


FIGURE 139 Configuration Status dialog box

12. Review the configuration. If you want to save a copy of the instructions, click the **Copy to Clipboard** button.

13. Click **Next** to confirm the configuration.

    The **Important Instructions** dialog box displays.

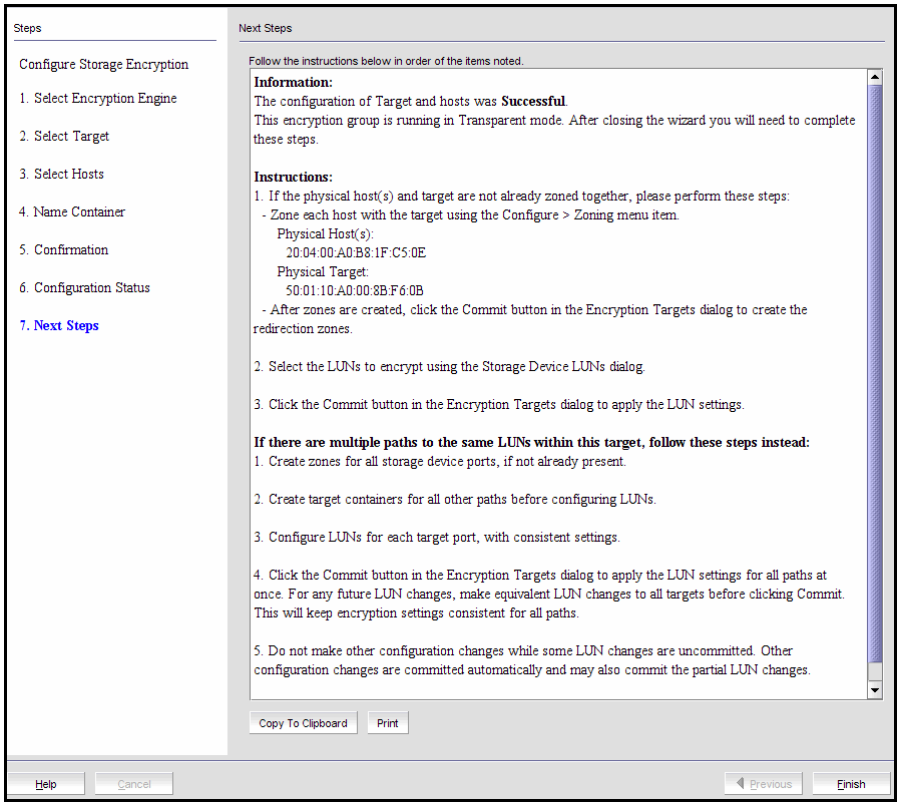

Steps
Configure Storage Encryption
1. Select Encryption Engine
2. Select Target
3. Select Hosts
4. Name Container
5. Confirmation
6. Configuration Status
7. Next Steps
Next Steps
Follow the instructions below in order of the items noted.
Information:
The configuration of Target and hosts was Successful.
This encryption group is running in Transparent mode. After closing the wizard you will need to complete these steps.
Instructions:
1. If the physical host(s) and target are not already zoned together, please perform these steps:
- Zone each host with the target using the Configure > Zoning menu item.
Physical Host(s):
20:04:00:A0:B8:1F:C5:0E
Physical Target:
50:01:10:A0:00:8B:F6:0B
- After zones are created, click the Commit button in the Encryption Targets dialog to create the redirection zones.
2. Select the LUNs to encrypt using the Storage Device LUNs dialog.
3. Click the Commit button in the Encryption Targets dialog to apply the LUN settings.
If there are multiple paths to the same LUNs within this target, follow these steps instead:
1. Create zones for all storage device ports, if not already present.
2. Create target containers for all other paths before configuring LUNs.
3. Configure LUNs for each target port, with consistent settings.
4. Click the Commit button in the Encryption Targets dialog to apply the LUN settings for all paths at once. For any future LUN changes, make equivalent LUN changes to all targets before clicking Commit. This will keep encryption settings consistent for all paths.
5. Do not make other configuration changes while some LUN changes are uncommitted. Other configuration changes are committed automatically and may also commit the partial LUN changes.
Copy To Clipboard
Print
Help
Cancel
Previous
Finish

FIGURE 140 Important Instructions dialog box

14. Review the instructions about post-configuration tasks you must complete after you close the wizard.
15. Click **Finish** to exit the **Configure Storage Encryption** wizard.

Configuring hosts for encryption targets

Use the **Encryption Target Hosts** dialog box to edit (add or remove) hosts for an encrypted target.

NOTE
Hosts are normally selected as part of the **Configure Storage Encryption** wizard but you can also edit hosts later using the **Encryption Target Hosts** dialog box.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select the encryption group, switch, or encryption engine containing the storage device to be configured.

3. Click **Encryption Targets**.

   The **Encryption Targets** dialog box displays.

4. Select a Target storage device from the list, and click **Hosts**.

   The **Encryption Target Hosts** dialog box displays. This dialog box lists configured hosts in a fabric.

5. Select one or more hosts in a fabric and move them to the **Selected Hosts** table.

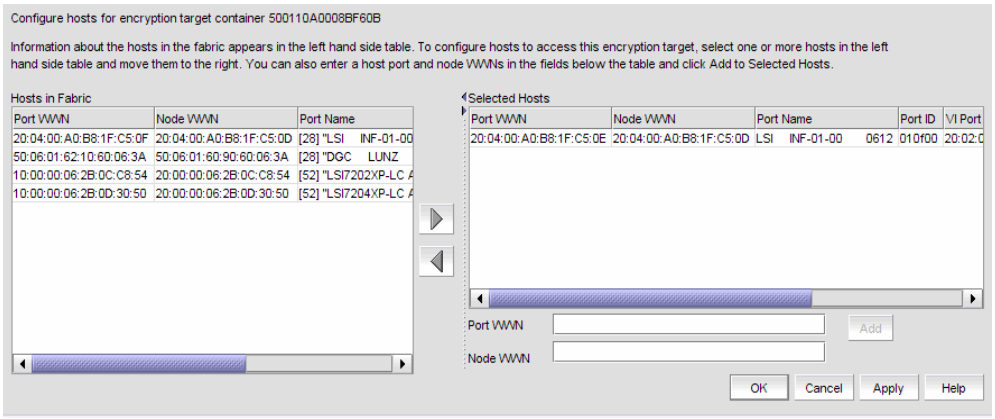


FIGURE 141 Encryption Target Hosts dialog box

Adding Target Disk LUNs for encryption

The **Encryption Target LUNs** dialog box lists configured LUNs. The displayed information is different for disk and tape devices. For example, tape volume and label information is included for tape devices. Initially, this list is empty.

NOTE
If you are using VMware virtualization software or any other configuration that involves mounted file systems on the LUN, you must enable first-time encryption when you create the LUN.

You configure a Crypto LUN by adding the LUN to the CryptoTarget container and enabling the encryption property on the Crypto LUN. You must add LUNs manually. The LUNs of the target which are not enabled for encryption must still be added to the CryptoTarget container with the **Clear Text** encryption mode option.

NOTE
When configuring a LUN with multiple paths, the same LUN policies must be configured on all the LUN's paths. If there are multiple paths to the same physical LUNs, then the LUNs are added to multiple target containers (one target per storage device port). See "Configuring encrypted storage in a multi-path environment" on page 362 for a multi-path configuration scenario.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select the encryption group, switch, or encryption engine containing the storage device to be configured.

3. Click **Encryption Targets**.

   The **Encryption Targets** dialog box displays.

4. Select a Target storage device from the list, and click **LUNs**.

   The **Encryption Target LUNs** dialog box displays. Initially, this list is empty. You must add LUNs manually.

   - Click the **Copy Settings** button to copy the data from a selected row to the next row.
   - Click the **Re-keying Details** button to launch the **LUN Re-keying Details** dialog of the selected LUN. When re-keying is in progress, the re-key completion percentage is updated automatically, at one minute intervals, until completion.

   NOTE
   You must configure LUNs on storage devices that are listed in the **Targets** dialog box for the host to access them, even if the LUNs are not encrypted.

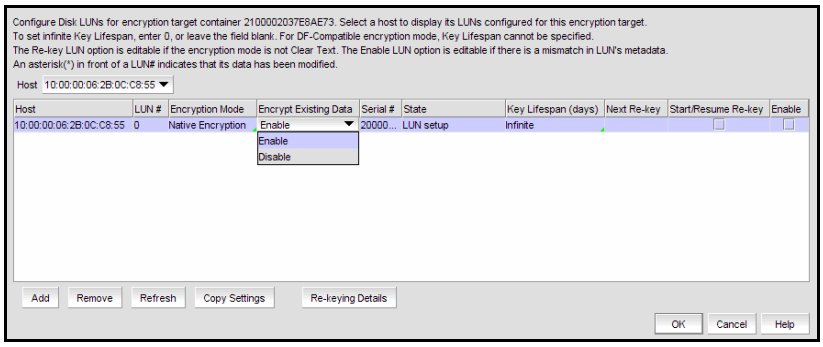


FIGURE 142 Encryption Target Disk LUNs dialog box

5. Click **Add**.

   The **Add LUNs** dialog box displays.

   This dialog box includes a table of all LUNs in the storage device that are visible to hosts. LUNs are identified by serial number, or by host WWN and LUN number. The LUN numbers may be different for different hosts.

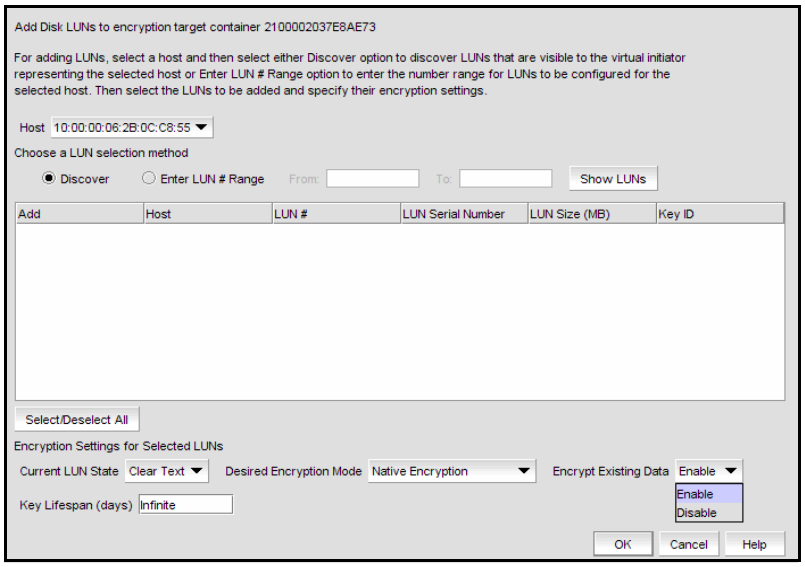

Add Disk LUNs to encryption target container 2100002037E8AE73
For adding LUNs, select a host and then select either Discover option to discover LUNs that are visible to the virtual initiator representing the selected host or Enter LUN # Range option to enter the number range for LUNs to be configured for the selected host. Then select the LUNs to be added and specify their encryption settings.
Host 10:00:00:06:2B:0C:C8:55
Choose a LUN selection method
Discover
Enter LUN # Range
From:
To:
Show LUNs
Add
Host
LUN #
LUN Serial Number
LUN Size (MB)
Key ID
Select/Deselect All
Encryption Settings for Selected LUNs
Current LUN State
Clear Text
Desired Encryption Mode
Native Encryption
Encrypt Existing Data
Enable
Enable
Disable
Key Lifespan (days)
Infinite
OK
Cancel
Help

FIGURE 143 Add Encryption Target Disk LUNs dialog box

6. Select a host from the **Host** list.

   There are two possible sources for the list of LUNs:

   - Specify a range of LUN numbers and click **Show LUNs**. This fills the table with dummy LUN information. This method works even if the target is offline. You can specify a range of LUN numbers only if a host is chosen from the list. If **All Hosts** is selected, you will not be able to specify a range but can discover LUNs.
   - Request discovery and click **Show LUNs**. The switch queries the target to determine which LUN numbers are visible to each configured host.

   When you select a specific host, only the LUNs visible to that host are displayed. If you select **All Hosts**, LUNs visible to all configured hosts are displayed. If a LUN is visible to multiple hosts, it is listed once for each host.

7. Select the check box in the **Add** column to add a LUN. You can use the **Select/De-select All** button to add all the LUNs, or to clear all selections.

8. Select the **Current LUN State**, which refers to data already on the LUN.

   - If the LUN is not encrypted, the correct value is **Clear Text**.
   - If the LUN was previously encrypted, select **Encrypted**.
   - If you disable the existing LUN data, the current LUN state setting does not matter.
   - The desired encryption mode.
   - The disposition for Existing Data.

   Warning: If the current LUN state is **Clear Text** and the desired state is encrypted, then a first time re-key will occur. If the current LUN state is **Encrypted** and the desired LUN state is **Clear Text**, a re-key will not occur. You may choose **Disable** from the Existing Data list to avoid this, but then all data on the LUN is lost.

   When changing an existing LUN to **Clear Text**, the data must be disabled, so it is recommended you back up the LUN's data first using a host-based application.

   NOTE
   For tape devices, the Existing Data components and the Current LUN State do not display.

9. If you want to enforce a **Re-keying Interval**, enter the number of days that you want to use a key before obtaining a new key. A value of 0 is equivalent to Infinite, which is the default.

   The **Re-keying Interval** field is editable only if the LUNs are encrypted. If **Clear Text** is selected as the encryption mode, **Re-Keying Interval** is disabled.

   NOTE
   For disk LUNs, expiration of the re-keying interval automatically triggers generation of a new key and starts a re-keying operation (reads and re-writes all data on the disk LUN).

10. Click **OK**.

11. Click **Commit** in the **Encryption Targets** dialog box when the LUNs have been added for all hosts that will access them.

    NOTE
    If there are other hosts that will access the same physical LUNs by way of other target ports (and thus other target containers), add the LUNs for the other hosts before you click **Commit**.

Adding Target Tape LUNs for encryption

You configure a Crypto LUN by adding the LUN to the CryptoTarget container and enabling the encryption property on the Crypto LUN. You must add LUNs manually. After you add the LUNs, you must specify the encryption settings.

When configuring a LUN with multiple paths, the same LUN policies must be configured on all the LUN's paths. If there are multiple paths to the same physical LUNs, then the LUNs are added to multiple target containers (one target per storage device port). See "Configuring encrypted storage in a multi-path environment" on page 362 for a multi-path configuration scenario.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select the encryption group, switch, or encryption engine containing the storage device to be configured.

3. Click **Encryption Targets**.

   The **Encryption Targets** dialog box displays.

4. Select a Target storage device from the list, and click **LUNs**.

   The **Encryption Target LUNs** dialog box displays.

5. Click **Add**.

   The **Add Encryption Target Tape LUNs** dialog box displays.

   This dialog box includes a table of all LUNs in the storage device that are visible to hosts. LUNs are identified by the Host world wide name, LUN number, and Volume Label Prefix number.

6. Select a host from the **Host** list.

   Before you encrypt a LUN you must select a host and then either discover LUNs that are visible to the virtual initiator representing the selected host, or enter a range of LUN numbers to be configured for the selected host.

7. Choose a LUN to be added to an encryption target container using one of the two following methods:

   - Discover. Click to identify the exposed logical unit number for a specified initiator. If you already know the exposed LUNs for the various initiators accessing the LUN, you can enter the range of LUNs using the alternative method.
   - Enter a LUN number range. Click to add a range of LUNs to be configured for the selected host. The LUN needed for configuring a Crypto LUN is the LUN that is exposed to a particular initiator.

8. Select the desired encryption mode.
   - If you change a LUN policy from **Native Encryption** or **DF-Compatible Encryption** to **Clear Text**, you disable encryption.
   - The LUNs of the target which are not enabled for encryption must still be added to the CryptoTarget container with the **Clear Text** encryption mode option.

   NOTE
   The Re-keying interval can only be changed for disk LUNs. For tape LUNs, expiration of the re-keying interval simply triggers the generation of a new key, to be used on future tape volumes. Tapes that are already made are not re-keyed. To re-key a tape, you would need to read the tape contents using a host application that decrypts the tape contents using the old key, and then re-write the tape, which re-encrypts the data with the new key.

9. Click **OK**.

   The selected tape LUNs are added to the encryption target container.

Configuring encrypted storage in a multi-path environment

This example assumes one host accessing one storage device using two paths:

- The first path is from host port A to target port A, using encryption engine A for encryption.
- The second path is from host port B to target port B, using encryption engine B for encryption.

Encryption engines A and B are in switches that are already part of encryption group *X*.

The following is the procedure for configuring this scenario using the Management application.

1. Zone host port A and target port A, using the **Configure > Zoning** dialog box.
2. Zone host port B and target port B, using the **Configure > Zoning** dialog box.
3. Open the **Encryption Center** dialog box by selecting **Configure > Encryption** from the Management application's main menu.
4. Click the **View By Encryption Groups** button to display the encryption groups.
5. Select encryption group *X*, then click the **Encryption Targets** button.
6. Click the **Add** button to start the **Configure Storage Encryption** wizard. Use the **Configure Storage Encryption** wizard to create a target container for encryption engine A with target port A and host port A.
7. Run the **Configure Storage Encryption** wizard again to create a target container for encryption engine B with target port B and host port B.

   Up to this point, the Management application has been automatically committing changes as they are made. The targets and hosts are now fully configured; only the LUN configuration remains.
8. In the **Encryption Targets** dialog box, select target port A, click **LUNs**, then click **Add**. Select the LUNs to be encrypted and the encryption policies for the LUNs.

9. Select target port B, click **LUNs**, then click **Add**. Select the LUNs to be encrypted and the encryption policies for the LUNs, making sure that the encryption policies match the policies specified in the other path.
10. Click **Commit** to make the LUN configuration changes effective in both paths simultaneously.

The Management application does not automatically commit LUN configuration changes. This allows matching changes made in a multi-path environment to be committed together, preventing cases where one path may be encrypting and another path is not encrypting, resulting in corrupted data. You must remember to click the **Commit** button after any LUN configuration changes, even in non-multi-path environments. The **Encryption Targets** dialog box displays a reminder if you attempt to close the dialog box without committing LUN configuration changes.

NOTE
There is a limit of 25 uncommitted LUN configuration changes. When adding more than 12 LUNs in a multi-path environment, repeat steps step 8 through step 10 above, adding only 12 LUNs to each target container at a time. Each commit operation, then, will commit 24 LUNs, 12 in each path.

Master keys

When an opaque key vault is used, a master key is used to encrypt the data encryption keys. The master key status indicates whether a master key is used and whether it has been backed up. Encryption is not allowed until the master key has been backed up.

Only the active master key can be backed up, and multiple backups are recommended. You can back up or restore the master key to the key vault, to a file, or to a recovery card set. A recovery card set is set of smart cards. Each recovery card holds a portion of the master key. The cards must be gathered and read together from a card reader attached to a PC running the Brocade SAN Management Application to restore the master key.

NOTE
It is very important to back up the master key because if the master key is lost, none of the data encryption keys can be restored and none of the encrypted data can be decrypted.

Active master key

The active master key is used to encrypt newly-created data encryption keys (DEKs) prior to sending them to a key vault to be stored. You can restore the active master key under the following conditions:

- The active master key has been lost, which happens if all encryption engines in the group have been zeroized or replaced with new hardware at the same time.
- You want multiple encryption groups to share the same active master key. Groups should share the same master key if the groups share the same key vault and tapes (or disks) are going to be regularly exchanged between the groups.

Alternate master key

The alternate master key is used to decrypt data encryption keys that were not encrypted with the active master key. Restore the alternate master key for the following reasons:

- To read an old tape that was created when the group used a different active master key.
- To read a tape (or disk) from a different encryption group that uses a different active master key.

Master key actions

Master key actions are as follows:

- **Backup master key**, which is enabled any time a master key exists.
- **Restore master key**, which is enabled when no master key exists or the previous master key has been backed up.
- **Create new master key**, which is enabled when no master key exists or the previous master key has been backed up.

Reasons master keys can be disabled

Master key actions are disabled if unavailable. There are several ways a master key can be disabled:

- The user does not have Storage Encryption Security permissions. See "Encryption user privileges" on page 315 for more information.
- The group leader is not discovered or managed by the Management application.

Saving the master key to a file

Use the following procedure to save the master key to a file.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select an encryption group from the tree, and click **Properties**.

   NOTE
   Master keys belong to the group and are managed from the group properties.

3. Select the **Security** tab.

4. Select **Backup Master Key** as the **Master Key Action**.

   The **Master Key Backup** dialog box displays, but only if the master key has already been generated.

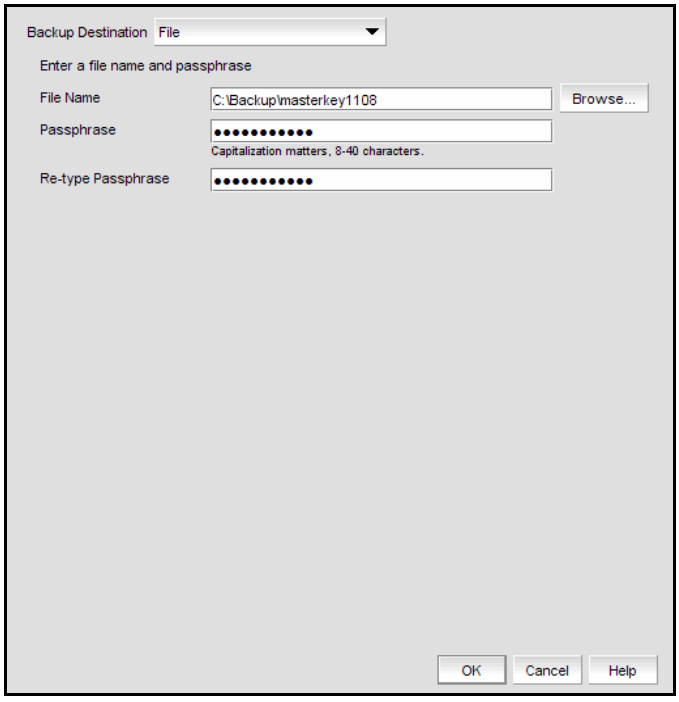


FIGURE 144 **Backup Destination (to file) dialog box**

5. Select **File** as the **Backup Destination**.
6. Enter a file name, or browse to the desired location.
7. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.
8. Re-type the passphrase for verification.
9. Click **OK**.

ATTENTION
Save the passphrase. This passphrase is required if you ever need to restore the master key from the file.

Saving a master key to a key vault

Use the following procedure to save the master key to a key vault.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select an encryption group from the tree, and click **Properties**.
3. Select the **Security** tab.
4. Select **Backup Master Key** as the **Master Key Action**.

   The **Backup Master Key for Encryption Group** dialog box displays.

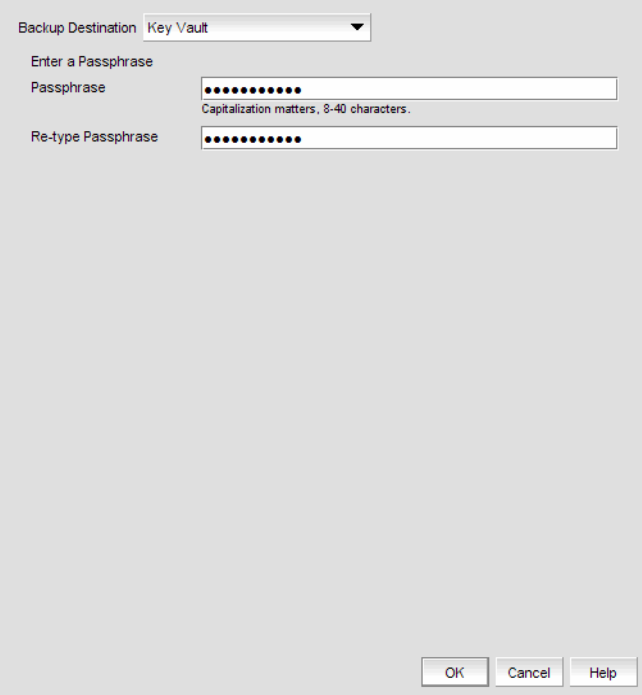


FIGURE 145 Backup Destination (to key vault) dialog box

5. Select **Key Vault** as the **Backup Destination**.
6. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.
7. Re-type the passphrase for verification.
8. Click **OK**.

   A dialog box displays that shows the **Key ID**.

9. Store both the **Key ID** and the passphrase in a secure place. Both will be required to restore the master key in the future. (The **Key ID** identifies the storage location in the key vault.)
10. Click **OK** after you have copied the key ID.

Saving a master key to a smart card set

A card reader must be attached to the SAN Management application PC to complete this procedure. Recovery cards can only be written once to back up a single master key. Each master key backup operation requires a new set of previously unused smart cards.

NOTE
Windows operating systems do not require smart card drivers to be installed separately; the driver is bundled with the operating system. You must install a smart card driver for Linux and Solaris operating systems, however. For instructions, see the *Data Center Fabric Manager Administrator's Guide*.

The key is divided between the cards in the card set. When the master key is backed up to a set of three cards, a minimum of two cards can be used together to restore the master key. When the master key is backed up to a set of five cards, a minimum of three cards can be used together to restore the master key. Backing up the master key to multiple recovery cards is the recommended and most secure option.

NOTE
When you write the key to the card set, be sure you write the full set without canceling. If you cancel, all the previously written cards become unusable, and you will need to discard them and create a new set.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select an encryption group from the tree, and click **Properties**.
3. Select the **Security** tab.
4. Select **Backup Master Key** as the **Master Key Action**.

   The **Backup Master Key for Encryption Group** dialog box displays.

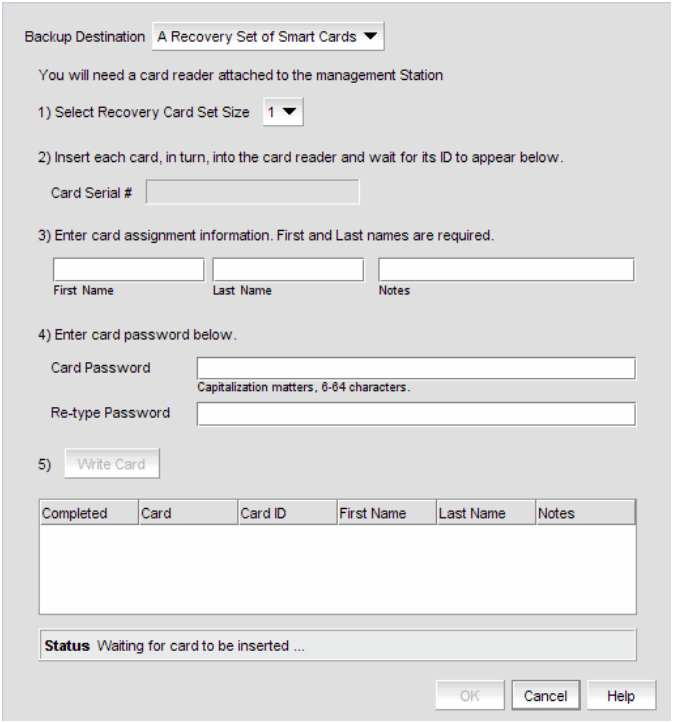


FIGURE 146 Backup Destination (to smart cards) dialog box

5. Select **A Recovery Set of Smart Cards** as the **Backup Destination**.
6. Enter the recovery card set size.
7. Insert the first blank card and wait for the card serial number to appear.
8. Run the additional cards needed for the set through the reader. As you read each card, the card ID displays in the **Card Serial#** field. Be sure to wait for the ID to appear.
9. Enter the mandatory last name and first name of the person to whom the card is assigned.
10. Type a Card **Password**.
11. Re-type the password for verification.
12. Record and store the password in a secure location.
13. Click **Write Card**.

    The dialog box prompts you to insert the next card, up to the number of cards specified in step 6.
14. Repeat step 7 through step 13 for each card.
15. Continue until you have written to all the cards in the set.
16. After the last card is written, click **OK** in the **Master Key Backup** dialog box to finish the operation.

Restoring a master key from a file

Use the following procedure to restore the master key from a file.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select an encryption group from the tree, and click **Properties**.
3. Select the **Security** tab.
4. Select **Restore Master Key** as the **Master Key Action**.

   The **Restore Master Key for Encryption Group** dialog box displays.

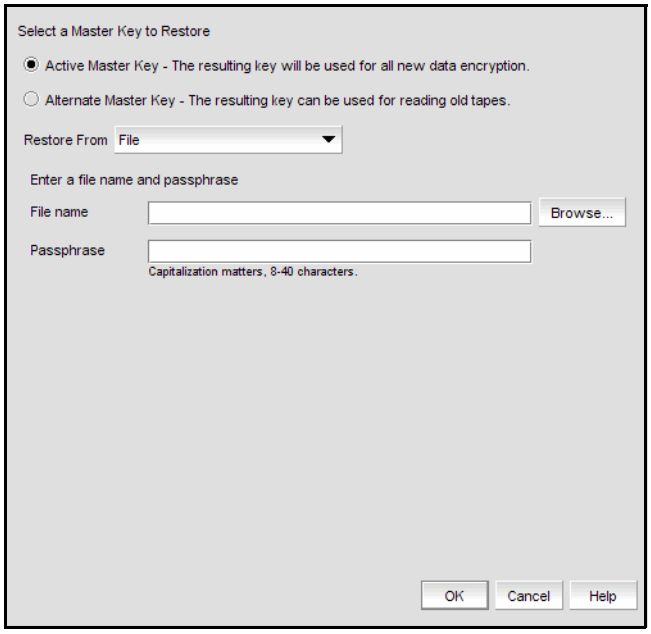

Select a Master Key to Restore
Active Master Key - The resulting key will be used for all new data encryption.
Alternate Master Key - The resulting key can be used for reading old tapes.
Restore From
File
Enter a file name and passphrase
File name
Browse...
Passphrase
Capitalization matters, 8-40 characters.
OK
Cancel
Help

FIGURE 147 Select a Master Key to Restore (from file) dialog box

5. Choose the active or alternate master key for restoration, as appropriate. Refer to "Active master key" on page 363 and "Alternate master key" on page 364 if you need more information on active and alternate master keys.
6. Select **File** as the **Restore From** location.
7. Enter a file name, or browse to the desired location.
8. Enter the passphrase. The passphrase that was used to back up the master key must be used to restore the master key.
9. Click **OK**.

Restoring a master key from a key vault

Use the following procedure to restore the master key from a key vault.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select an encryption group from the tree, and click **Properties**.
3. Select the **Security** tab.
4. Select **Restore Master Key** as the **Master Key Action**.

   The **Restore Master Key for Encryption Group** dialog box displays.

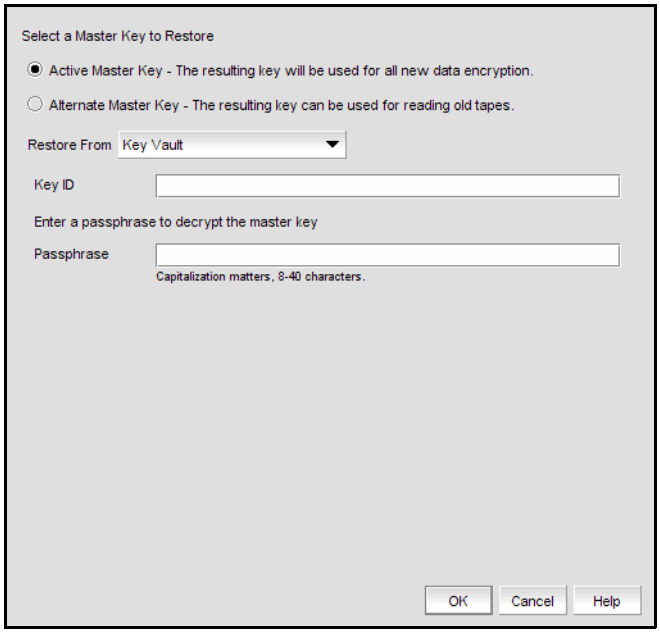

Select a Master Key to Restore
Active Master Key - The resulting key will be used for all new data encryption.
Alternate Master Key - The resulting key can be used for reading old tapes.
Restore From
Key Vault
Key ID
Enter a passphrase to decrypt the master key
Passphrase
Capitalization matters, 8-40 characters.
OK
Cancel
Help

FIGURE 148 Select a Master Key to Restore (from key vault) dialog box

5. Choose the active or alternate master key for restoration, as appropriate. Refer to "Active master key" on page 363 and "Alternate master key" on page 364 if you need more information on active and alternate master keys.
6. Select **Key Vault** as the **Restore From** location.
7. Enter the key ID of the master key that was backed up to the key vault.
8. Enter the passphrase. The passphrase that was used to back up the master key must be used to restore the master key.
9. Click **OK**.

Restoring a master key from a smart card set

A card reader must be attached to the SAN Management application PC to complete this procedure.

Use the following procedure to restore the master key from a set of smart cards.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Select an encryption group from the tree, and click **Properties**.
3. Select the **Security** tab.
4. Select **Restore Master Key** as the **Master Key Action**.

   The **Restore Master Key for Encryption Group** dialog box displays.

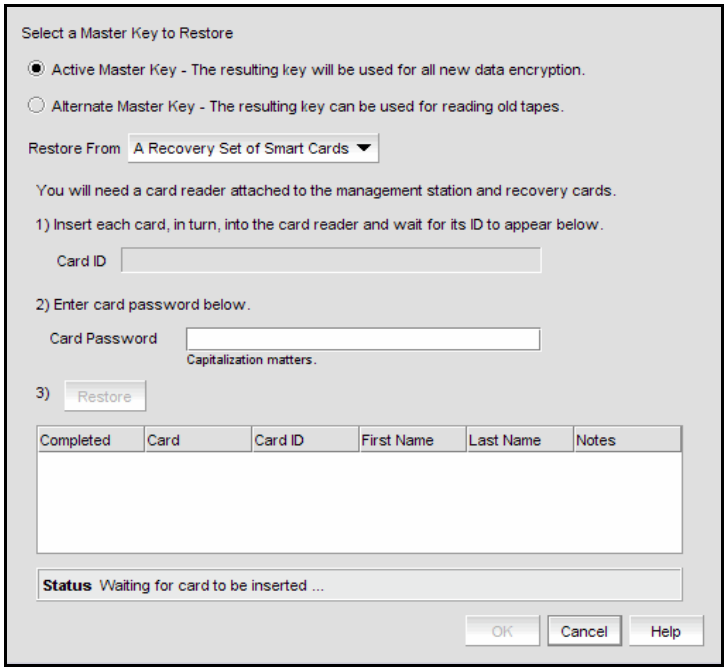

Select a Master Key to Restore
Active Master Key - The resulting key will be used for all new data encryption.
Alternate Master Key - The resulting key can be used for reading old tapes.
Restore From
A Recovery Set of Smart Cards
You will need a card reader attached to the management station and recovery cards.
1) Insert each card, in turn, into the card reader and wait for its ID to appear below.
Card ID
2) Enter card password below.
Card Password
Capitalization matters.
3)
Restore
Completed
Card
Card ID
First Name
Last Name
Notes
Status Waiting for card to be inserted ...
OK
Cancel
Help

FIGURE 149 Select a Master Key to Restore (from a recovery set of smart cards) dialog box

5. Choose the active or alternate master key for restoration, as appropriate. Refer to "Active master key" on page 363 and "Alternate master key" on page 364 if you need more information on active and alternate master keys.
6. Select **A Recovery Set of Smart Cards** as the **Restore From** location.
7. Insert the recovery card containing a share of the master key that was backed up earlier, and wait for the card serial number to appear.
8. Enter the password that was used to create the card. After five unsuccessful attempts to enter the correct password, the card becomes locked and unusable.
9. Click **Restore**.

   The dialog box prompts you to insert the next card, if needed.

10. Insert the next card, and repeat step 8 and step 9.
11. Continue until all the cards in the set have been read.
12. Click **OK**.

Creating a new master key

Though it is generally not necessary to create a new master key, you may be required to create one due to circumstances such as the following:

- The previous master key has been compromised.
- Corporate policy might require a new master key every year for security purposes.

When you create a new master key, the former active master key automatically becomes the alternate master key.

The new master key cannot be used (no new data encryption keys can be created, so no new encrypted LUNs can be configured), until you back up the new master key. After you have backed up the new master key, it is strongly recommended that all encrypted disk LUNs be re-keyed. Re-keying causes a new data encryption key to be created and encrypted using the new active master key, thereby removing any dependency on the old master key.

1. Select **Configure > Encryption**.
2. Select an encryption group from the tree and click **Properties**.
3. Select the **Security** tab.
4. Select **Create a New Master Key** from the list.

   The **Confirm Master Key Creation** dialog box displays.

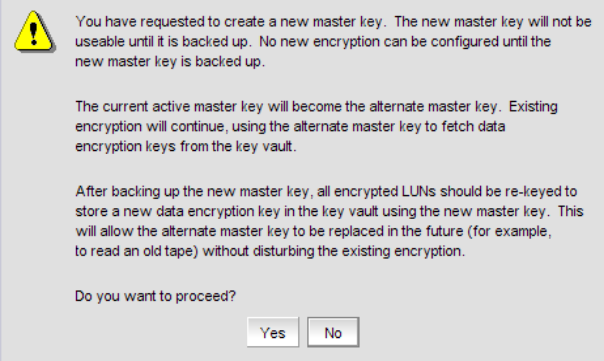

You have requested to create a new master key. The new master key will not be useable until it is backed up. No new encryption can be configured until the new master key is backed up.
The current active master key will become the alternate master key. Existing encryption will continue, using the alternate master key to fetch data encryption keys from the key vault.
After backing up the new master key, all encrypted LUNs should be re-keyed to store a new data encryption key in the key vault using the new master key. This will allow the alternate master key to be replaced in the future (for example, to read an old tape) without disturbing the existing encryption.
Do you want to proceed?
Yes
No

FIGURE 150 Confirm master key creation dialog box

5. Read the information, and click **Yes** to proceed.

Zeroizing an encryption engine

Zeroizing is the process of erasing all data encryption keys and other sensitive encryption information in an encryption engine. You can zeroize an encryption engine manually to protect encryption keys. No data is lost because the data encryption keys for the encryption targets are stored in the key vault.

Zeroizing has the following effects:

- All copies of data encryption keys kept in the encryption switch or encryption blade are erased.
- Internal public and private key pairs that identify the encryption engine are erased and the encryption switch or the encryption blade is in the FAULTY state.
- All encryption operations on this engine are stopped and all virtual initiators (VI) and virtual targets (VT) are removed from the fabric's name service.
- The key vault link key (for NetApp LKM key vaults) or the master key (for other key vaults) is erased from the encryption engine.

  Once enabled, the encryption engine is able to restore the necessary data encryption keys from the key vault when the link key (for the NetApp Lifetime Key Management application) or the master key (for other key vaults) are restored.
- If the encryption engine was part of an HA cluster, targets fail over to the peer which assumes the encryption of all storage targets. Data flow will continue to be encrypted.
- If there is no HA backup, host traffic to the target will fail as if the target has gone offline. The host will not have unencrypted access to the target. There will be no data flow at all because the encryption virtual targets will be offline.

NOTE
Zeroizing an engine affects the I/Os but all target and LUN configuration is intact. Encryption target configuration data is not deleted.

You can zeroize an encryption engine only if it is enabled (running) or disabled, but ready to be enabled. If the encryption engine is not in one of these states, an error message displays.

When using a NetApp LKM key vault, if all the encryption engines in a switch are zeroized, the switch loses the link key required to communicate with the LKM vault. After the encryption engines are rebooted and re-enabled, you must use the CLI to create new link keys for the switch.

When using an opaque key vault, if all the encryption engines in an encryption group are zeroized, the encryption group loses the master key required to read data encryption keys from the key vault. After the encryption engines are rebooted and re-enabled, you must restore the master key from a backup copy, or alternatively you can also generate a new master key and back it up. Restoring the master key from a backup copy or generating a new master key and backing it up indicates that all previously generated DEKs will not be decryptable, unless the original master key used to encrypt them is restored.

Use the **Restore Master key** wizard from the **Encryption Group Properties** dialog box to restore the master key from a backup copy.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.
2. Select the encryption engine, and then click **Zeroize**.

   A confirmation dialog box describing consequences and actions required to recover launches.

3. Initialize the encryption engine.

   An automatic power cycle and reboot occurs on the encryption blade and encryption switch.

4. Enable the encryption engine using the **Switch Encryption Properties** dialog box:

   a. Select the encryption engine from the **Encryption Center** dialog box.

   b. Click the **Properties** button.

      The **Switch Encryption Properties** dialog box displays.

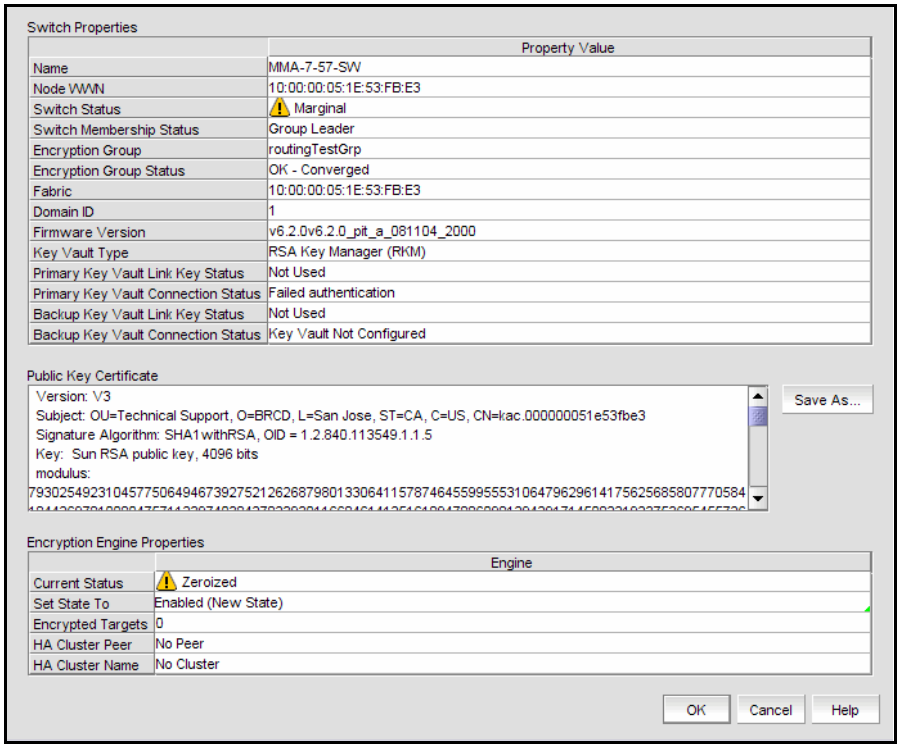


FIGURE 151 Switch Encryption Properties dialog box

   c. Select **Enabled (New State)** from the **Set State To** list for each encryption engine.

   d. Click **OK**.

Tracking Smart Cards

Smart Cards, which are credit card-sized cards that contain a CPU and persistent memory, are a secure way to back up and restore a master key. Using Smart Cards is optional. Master keys can also be backed up to a file or key vaults and are only used for encryption groups using RKM or HP SKM key vaults.

Even if an encryption group is deleted, the smart cards are still displayed. You must manually delete them.

Use the **Smart Card Asset Tracking** dialog box to track Smart Card details.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays.

2. Click **Smart Card Tracking**.

   The **Smart Card asset tracking** dialog box displays.

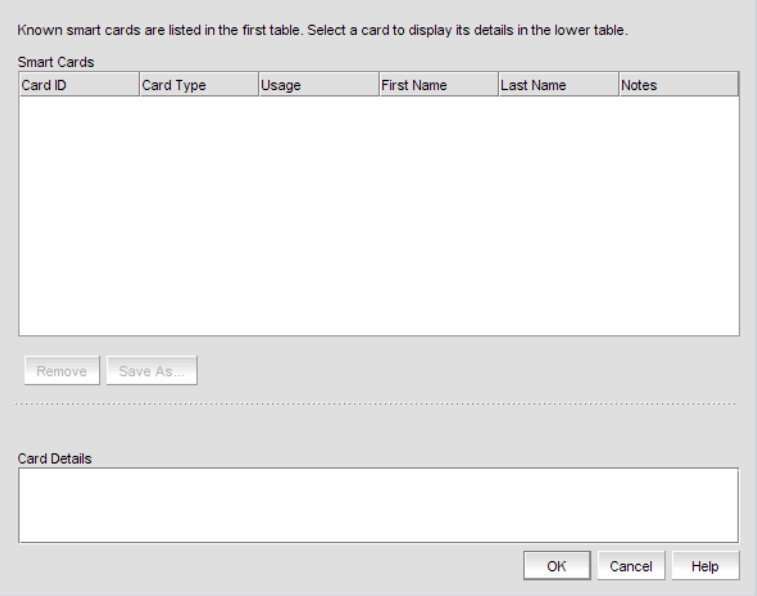


FIGURE 152 Smart Card asset tracking dialog box

Clicking the **Remove** button removes a selected smart card from the Management application database. You can remove smart cards to keep the **Smart Cards** table at a manageable size, but removing the card from the table does not invalidate it. The Smart Card can still be used.

Clicking the **Save As** button saves the entire list of smart cards to a file. The available formats are comma-separated values (.csv) and HTML files (.html).

Encryption-related acronyms in log messages

Fabric OS log messages related to encryption components and features may have acronyms embedded that require interpretation. Table 35 lists some of those acronyms.

TABLE 35 Encryption Acronyms

Acronym	Name
EE	Encryption Engine
EG	Encryption Group
HAC	High Availability Cluster

Chapter

13

Zoning

In this chapter

- Zoning overview 377
- Zoning configuration 379
- Traffic isolation zoning 397
- Zoning administration 402

Zoning overview

Zoning defines the communication paths in a fabric. A zone is a collection of initiator and target ports within the SAN. The ports in a zone can only communicate with other ports in that zone. However, ports can be members of more than one zone.

Zoning is a fabric management service that can be used to create logical subsets of devices within a SAN and enable partitioning of resources for management and access control purposes. Zoning allows only members of a zone to communicate within that zone. All others attempting to access from outside the zone are rejected, hence zoning also provides a security function.

Zoning provides software zoning controlled at the Node World Wide Name (nWWN) level assisted by the name server of a switch. Depending on the vendor, it also supports Domain/Port zoning and Fabric Address zoning in a fabric without any router. Domain/Port zoning is not supported when the fabric is in McDATA Open Mode (Interop Mode 3).

Special zones

Fabric OS has the following types of zones:

- Zones

  Enable you to partition your fabric into logical groups of devices that can access each other. These are “regular” or “normal” zones. Unless otherwise specified, all references to zones in this chapter refer to these regular zones.

- Frame redirection zones

  Re-route frames between an initiator and target through a Virtual Initiator and Virtual Target for special processing or functionality, such as for storage virtualization or encryption. See “Redirection zones” on page 335 for more information.

- QoS zones

  Assign high or low priority to designated traffic flows. QoS zones are normal zones with additional QoS attributes that you select when you create the zone.

- Traffic Isolation zones (TI zones)

  Isolate inter-switch traffic to a specific, dedicated path through the fabric. See "Traffic isolation zoning" on page 397 for more information.

Online zoning

Online zoning allows you to do the following:

- View both defined and active zone information in the fabric.
- Create and modify zones and zone configurations in the software zone database.
- Activate a zone configuration in order to publish the zone information in the selected fabric.
- Deactivate the current active zone configuration.
- Configure zoning policies in the selected fabric.
- Generate zoning reports for the fabric.

Accessing zoning

You can access Zoning from the main screen of the Management application using any of the following methods:

- Select **Configure > Zoning > Fabric**.
- Click the **Zoning** icon on the toolbar.
- Right-click a port, switch, switch group, or fabric in the device list and select **Zoning**.
- Right-click a port, switch, switch group, or fabric in the Connectivity Map and select **Zoning**.

Zoning naming conventions

The naming rules for zone names, zone aliases, and zone configuration names vary with the type of fabric.

The following conventions apply to Fibre Channel fabrics:

- Names are case sensitive in McDATA Open Mode. However, names are *not* case sensitive in Brocade Native Mode or McDATA Fabric Mode.
- Zone, alias, and configuration names cannot begin with "red_", "lsan_red_", or "d__efault__". Zone configuration names cannot begin with "r_e_d_i_r_c__fg". These prefixes are reserved.
- Names cannot begin with a numeric character or a special character.
- Recommended character limit: 64 characters.
- Duplicate names are not allowed between zones, zone aliases, and zone configurations within a zone database.

Invalid zoning name

If you enter an invalid zone or zone configuration name, an error or warning message displays depending on the type of fabric you are trying to zone:

- For FC Fabrics, if an invalid name is entered for a zone or zone configuration, the application displays a warning message. If there is a naming violation according to the vendor, the Switch returns the error message for the exact information along with the zone configuration activation failure message.

Zoning configuration

At a minimum, zoning configuration entails creating zones and zone members. However, you can also create zone aliases, zone configurations, and zone databases. You can define multiple zone configurations, deactivating and activating individual configurations as your needs change. Zoning configuration can also involve enabling or disabling safe zoning mode and the default zone.

Configuring zoning for the SAN

The following procedure provides an overview of the steps you must perform to configure zoning for the SAN.

Note that for any zoning-related procedure, changes to a zone database are not saved until you click **OK** or **Apply** on the **Zoning** dialog box. If you click **Cancel** or the close button (X), no changes are saved.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. If you want to show all the discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
5. Create the zones.

   For specific instructions, refer to “Creating a new zone” on page 380.

6. Add members to each zone.

   For specific instructions, refer to “Adding members to a zone” on page 381.

7. Create a zone configuration.

   For specific instructions, refer to “Creating a zone configuration” on page 389.

8. Activate the zone configuration.

   For specific instructions, refer to “Activating a zone configuration” on page 391.

9. Set zoning policies for FC fabrics, if necessary.

   For specific instructions, refer to "Enabling or disabling the default zone for fabrics" on page 385 and "Enabling or disabling safe zoning mode for fabrics" on page 386.

10. Click **OK** or **Apply** to save your changes.

    A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Creating a new zone

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click **New Zone**.

   A new zone displays in the **Zones** list.

5. Type the desired name for the zone.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 378.

6. (Optional—Fabric OS only) Set the QoS for the zone by right-clicking the zone and selecting **QoS > *Priority_Level*** (High, Medium, or Low).

   NOTE
   QoS priority support is available for zones with WWN or Domain,Index (D,I) members.

   QoS zones using D,I notation cannot be created if any of the switches in the fabric are running Fabric OS versions earlier than 6.3.0.

   The zone name is automatically renamed to QoS*X_Zone_Name*, where X is the priority level (H—High, M—Medium, or L—Low) and *Zone_Name* is the name you entered for the zone.

7. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

   If the zone is empty, a warning message displays.

Viewing zone properties

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the zone you want to review in the **Zones** list and select **Properties**.

   The **Zone Properties** dialog box displays.

5. Review the zone properties.

   Depending on what type of zone you selected, the following information is included in the zone properties:

   - **Zone Name**—The name of the zone.
   - **Zone Configs Containing This Zone**—The number of zone configurations to which this zone belongs.
   - **Total Zone Members**—The number of zone members in the selected zone.
   - **Number of Aliases**—The number of aliases in this zone.
   - **Zone Members Contained by Aliases**—The number of zone members in the selected alias.
   - **Configure Status** (TI Zone only)—(Fabric OS only) Whether or not the TI zone is enabled.
   - **Configure Failover** (TI Zone only)—(Fabric OS only) Whether or not the TI zone failover is enabled.
   - **Status**—The status of the selected zone.

6. Click **OK** to close the **Zone Properties** dialog box.

Adding members to a zone

Use this procedure to add a member to a zone when the member is listed in the **Potential Members** list of the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. If you want to show all the discovered fabrics in your fabric group in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
5. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)

6. Select an option from the **Type** list.

   By default, the first time you launch the **Zoning** dialog box for a Zoning Scope, the **Potential Members** list displays valid members using the following rules:

   - If you select the **World Wide Name** type, the valid members display by the Attached Ports.
   - If you select the **Domain/Port Index** type, the valid members display by the ALL Product Ports (both occupied and unoccupied). This option is available for FC fabrics only.
   - If you select the **Alias** type, the valid members display by the device Alias.

7. Select one or more members to add to the zone in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member. To add all ports on a device, select the device.)
8. Click the right arrow between the **Potential Members** list and **Zones** list to add the selected members to the zone.

   A message may display informing you that one or some of the selected potential members cannot be zoned. Click **OK** to close the message box. Reconsider your selections and make corrections as appropriate.

9. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Creating a new member in a zone by WWN

Use this procedure to add a member to a zone when the member is not listed in the **Potential Members** list of the **Zone DB** tab.

For instructions to add a member to a zone when the member is listed in the **Potential Members** list, refer to the procedure "Adding members to a zone" on page 381.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)
5. Click **New Member**.

   The **Add Zone Member** dialog box displays.

6. Select **World Wide Name** from the **Member Type** list.

7. Add the new member by port name by completing the following steps.
   a. Select the **Existing End Device Node/Port Name** option.
   b. Select a port name from the list.

   OR

   Add the new member by port WWN by completing the following steps.
   a. Select the **End Device Node/Port WWN** option.
   b. Enter a port WWN in the **End Device Node/Port WWN** field.

      If you enter a WWN that has been used by a discovered device, a message displays informing you of this and instructing you to enter a port WWN. Click **OK** to close the message box and enter an appropriate WWN.
   c. (*Optional*) Click the **Assign Name** check box and enter a name in the field.

      If a name was previously assigned, the name appears in the field and a message displays asking whether you want to overwrite the existing name. Click **Yes** to continue and assign a new name, or **No** to decline and close the message box.
8. Click **OK** to save your changes and close the **Add Zone Member** dialog box.

   OR

   Click **Apply** to save your changes and keep the **Add Zone Member** dialog box open so you can add more new members. Repeat steps 5, 6 and 7 as many times as needed, and proceed to step 8 when appropriate.
9. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Creating a new member in a zone by domain, port index

Use this procedure to add a member to a zone when the member is not listed in the **Potential Members** list of the **Zone DB** tab.

For instructions to add a member to a zone when the member is listed in the **Potential Members** list, refer to the procedure "Adding members to a zone" on page 381.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)
5. Click **New Member**.

   The **Add Zone Member** dialog box displays.

6. Select **Domain, Port Index** from the **Member Type** list.
7. Add the new member by port name by completing the following steps.
   a. Select the **Existing Switch Port Name** option.
   b. Select a name from the list.

   OR

   Create a new member by domain and port index by choosing one of the following options:

   - Select the **Domain, Port Index (decimal)** option and enter domain and port values in the fields.
   - Select the **Domain, Port Index (hex)** option and enter domain and port values in the fields.
8. Click **OK** to save your changes and close the **Add Zone Member** dialog box.

   OR

   Click **Apply** to save your changes and keep the **Add Zone Member** dialog box open so you can add more new members. Repeat steps 5, 6 and 7 as many times as needed, and proceed to step 8 when appropriate.
9. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Creating a new member in a zone by alias

Use this procedure to add a member to a zone when the member is not listed in the **Potential Members** list of the **Zone DB** tab. For instructions to add a member to a zone when the member is listed in the **Potential Members** list, refer to the procedure "Adding members to a zone" on page 381.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)
5. Click **New Member**.

   The **Add Zone Member** dialog box displays.
6. Select **Alias** from the **Member Type** list.

7. Add the new member by alias name by completing the following steps.
   a. Select the **Existing Alias** option.
   b. Select an alias from the list.

   OR

   Create a new alias by completing the following steps.
   a. Select the **New Alias** option.
   b. Enter a name in the **New Alias** field.
   c. Assign the alias by choosing one of the following options:
      - Select the **WWN** option and enter the WWN in the field.
        If you enter a WWN that has been used by a discovered device, a message displays informing you of this and instructing you to enter a port WWN. Click **OK** to close the message box and enter an appropriate WWN.
      - Select the **Domain, Port Index (decimal)** option and enter domain or port values in the fields.
      - Select the **Domain, Port Index (hex)** option and enter domain or port values in the fields.
8. Click **OK** to save your changes and close the **Add Zone Member** dialog box.

   OR

   Click **Apply** to save your changes and keep the **Add Zone Member** dialog box open so you can add more new members. Repeat steps 5, 6 and 7 as many times as needed, and proceed to step 8 when appropriate.
9. Click **OK** or **Apply** to save your changes.
   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Enabling or disabling the default zone for fabrics

Use this procedure to enable or disable the default zone for FC and Router fabrics.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Select the zoning database you want from the **Zone DB** list.

5. Click **Zoning Policies**.

   The **Zoning Policies** dialog box displays.

   NOTE
   The format and content of this dialog box vary slightly depending on Interop Mode, the target selected in the **Zoning Scope** list, and whether safe zoning mode is enabled. If safe zoning mode is enabled, the **Default Zone** button is disabled. If you want to enable the default zone, you need to disable the safe zoning mode.

6. Make sure the appropriate fabric is named on the **Zoning Policies** dialog box.
7. Perform one of the following actions based on the task you want to complete:
   - To enable the default zone, click **Enable**, and then click **OK**.
   - To disable the default zone, click **Disable**, and then click **OK**.

   The **Zoning Policies** dialog box closes and the **Zone DB** tab displays.
8. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Enabling or disabling safe zoning mode for fabrics

Use this procedure to enable or disable Safe Zoning Mode for FC and Router fabrics.

NOTE
Safe Zoning Mode is available only on devices running in McDATA Fabric Mode and, for pure EOS fabrics, in McDATA Open Mode.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Click **Zoning Policies**.

   The **Zoning Policies** dialog box displays.

   NOTE
   The format and content of this dialog box vary slightly depending on Interop Mode and the target selected in the **Zoning Scope** list.

5. Make sure the appropriate fabric is named on the **Zoning Policies** dialog box.
6. Perform one of the following actions based on the task you want to complete:
   - To enable the default zone, click **Enable**, and then click **OK**.
   - To disable the default zone, click **Disable**, and then click **OK**.

7. Click **OK** to apply your changes and close the **Zoning Policies** dialog box.
8. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Creating a new zone alias

An alias is a logical group of port index numbers and WWNs. Specifying groups of ports or devices as an alias makes zone configuration easier, by enabling you to configure zones using an alias rather than inputting a long string of individual members. You can specify members of an alias using the following methods:

- Identifying members by switch domain and port index number pair (for example, 2, 20).
- Identifying members by device node and device port WWNs.

Use this procedure to create a zone alias.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.
4. Select **Alias** from the **Type** list.
5. Click **New Alias**.

   The **New Alias** dialog box displays.
6. Type the desired name for the alias in the **Alias Name** field.
7. Select **WWN** or **Domain, Port Index** to choose how to display the objects in the **Potential Members** list.
8. Show all discovered fabrics in the **Potential Members** list by right-clicking in the **Potential Members** list and selecting **Display All**.
9. Select one or more members that you want to add to the alias in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)
10. Click the right arrow between the **Potential Members** list and **Selected Member(s)** list to add the selected members to the alias.
11. Click **OK** on the **New Alias** dialog box to save your changes.
12. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Editing a zone alias

Use this procedure to edit a zone alias.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Select the alias you want to edit in the **Alias** list.

5. Click **Edit**.

   The **Edit Alias** dialog box displays.

6. Add members to the alias by completing the following steps.

   a. Select **WWN** or **Domain, Port Index** to choose how to display the objects in the **Potential Members** list.

   b. Show all discovered fabrics in the **Potential Members** list by right-clicking in the **Potential Members** list and selecting **Expand All**.

   c. Select one or more members that you want to add to the alias in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)

   d. Click the right arrow between the **Potential Members** list and **Selected Member(s)** list to add the selected members to the alias.

7. Remove members from the alias by completing the following steps.

   a. Select one or more members that you want to remove from the alias in the **Selected Member(s)** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)

   b. Click the left arrow between the **Potential Members** list and **Selected Member(s)** list to remove the selected members to the alias.

8. Click **OK** on the **Edit Alias** dialog box to save your changes.

9. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Removing an object from a zone alias

Use this procedure to remove an object (by WWN or Domain, Port Index) from a zone alias.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select **Alias** from the **Type** list.

4. Show all objects in the **Alias** list by right-clicking a object and selecting **Tree > Expand All**.

5. Select one or more objects that you want to remove from the alias in the **Alias** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)

   You can select objects from different zone aliases.

6. Right-click one of the selected objects and select **Remove.**

   To selected objects are removed from the associated **Zone Alias**.

7. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Exporting zone aliases

Use this procedure to export a zone alias.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Click **Export.**

   The **Export Alias** dialog box displays.
5. Browse to the location to which you want to export the zone alias data.
6. Enter a name for the export file in the **File Name** field.
7. Click **Export Alias**.
8. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Renaming a zone alias

Use this procedure to rename a zone alias.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Right-click the zone alias you want to rename and select **Rename.**
5. Edit the name and press **Enter**.
6. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Creating a zone configuration

Use this procedure to create a new zone configuration.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Click **New Config**.

   A new configuration displays in the **Zone Configs** list.

5. Enter a name for the zone configuration.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 378.

6. Press **Enter**.

   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the zone creation.

7. Add zones to the zone configuration.

   For step-by-step instructions, refer to "Adding zones to zone configurations" on page 391.

8. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Viewing zone configuration properties

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Potential Members** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

4. Right-click the zone configuration you want to review in the **Zone Configs** list and select **Properties**.

   The **Zone Config Properties** dialog box displays.

5. Review the zone configuration properties.

   The following information is included in the zone properties:

   - **Zone Config Name**—The name of the selected zone configuration.
   - **Number of Zones**—The number of zones in the selected zone configuration.
   - **Total Zone Members**—The total number of zone members in the selected zone configuration.
   - **Unique Zone Members**—The total number of zone members that are unique in the zone configuration.
   - **Status**—The status of the selected zone configuration (active or not active).

6. Click **OK** to close the **Zone Config Properties** dialog box.

Adding zones to zone configurations

Use this procedure to add one or more zones to a zone configuration.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zone configurations to which you want to add zones in the **Zone Configs** list. (Press **SHIFT** or **CTRL** and click each zone configuration name to select more than one zone configuration.)

5. Select one or more zones to add to the zone configurations in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)

6. Click the right arrow between the **Zones** list and **Zone Configs** list to add the zones to the zone configurations.

7. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Activating a zone configuration

For FC Fabrics and Router Fabrics, when a zone configuration is active, its members can communicate with one another. Only one zone configuration can be active at any given time.

When you initiate activation of a zone configuration, a number of checks are performed on the zone configuration. These checks are performed before the **Activate Zone Config** dialog box is displayed, and look for the following problems:

- Zone and zone configuration name violations
- Zoning configuration violations
- Zone configuration change limit violations

For FC Fabrics, during zone configuration activation, the total number of zone members in each zone and in the zone configuration are checked against the limits imposed by the firmware and hardware product. If the limits are exceeded, a message is displayed informing you of the exceeded limits as well as the zone configuration failure information. Click **OK** to close the message box, and take appropriate action to meet the limits.

When a zone configuration is activated, the entire zone database is sent to the fabric, except for Interop Mode 3, when only the active configuration information is sent to the fabric.

NOTE
Only one server should be run at a time (actual servers performing discovery) or logon conflicts may occur. Also, activation speeds may differ depending on the hardware vendor and type of zoning used.

There are several conditions that could cause the **Activate** button to be unavailable. They include the following:

- If you do not have access privileges to activate zone configurations, the **Activate** button on the **Zone DB** tab will be unavailable. You will not be able to activate a zone configuration unless your access privileges are redefined.
- The fabric is not manageable.
- You do not have Read/Write or Activate privilege for the selected fabric and the selected zone database (for FC Fabric only).
- The selected fabric is not supported by the Management application.
- The selected fabric is no longer discovered.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone configuration you want to activate in the **Zone Configs** list.
5. Click **Activate**.

   The Management application begins performing various checks. Note the following events that may occur:

   - For FC fabrics, and depending on the characters included in the name you gave to this zone configuration, a message may display informing you the name contains characters that are not accepted by some switch vendors and asking whether you want to proceed. Click **Yes** to continue and proceed to the **Activate Zone Config** dialog box, or click **No** to cancel the activation and consider your naming options.
   - For FC fabrics, when the total number of zones and zone members defined exceeds the limit recommended for the system firmware, a warning message displays informing you of this fact and asking whether you want to proceed. Consider carefully whether you want to continue with the zone configuration activation. The limits are set to ensure stable fabrics; if you proceed, you may undermine the stability of your fabric. Click **Yes** to continue and proceed to the **Activate Zone Config** dialog box, or click **No** to cancel the activation.

     You can then click **Cancel** to close the **Activate Zone Config** dialog box, reduce the number of zones or zone members on the **Zone DB** tab, and then return to this procedure to activate the zone configuration.

   - For FC fabrics, if a limit on the number of zone database changes is enforced and you have exceeded this limit, a message displays informing you that activation is not allowed.

6. Review the information in the **Activate Zone Config** dialog box and make sure the selected zone configuration is the one you want to activate. Also, select or clear the **Generate a report** check box as required.

7. Click **OK** to activate the zone configuration.

   A message box displays informing you that the zones and zone configurations you change will be saved in the zone database and asking whether you want to proceed. Click **Yes** to confirm the activation, or **No** to cancel the activation.

   When you click **Yes**, a busy window displays indicating the activation is in progress. A status field informs you whether the activation succeeded or failed. When it succeeds, icons for the active zone configuration and its zones display green. When it fails, the message includes the reason for the failure.

8. Click **OK** to continue.

   The **Activate Zone Config** dialog box is closed and the **Zone DB** tab displays.

9. Click **OK**.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Deactivating a zone configuration

Use this procedure to deactivate the active zone configuration.

There are several conditions that could cause the **Deactivate** button to be unavailable. They include the following:

- There is no active zone configuration in the selected fabric.
- The fabric is not manageable.
- You do not have Read/Write or Activate privilege for the selected fabric and the selected zone database (for FC Fabric only).
- The selected fabric is not supported by the Management application.
- The selected fabric is no longer discovered.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Active Zone Config** tab.
3. Select an FC fabric from the **Active Zone Config** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click **Deactivate**.
5. Click **Yes** on the confirmation message.

   If the deactivation succeeded, the zone configuration no longer displays in the **Active Zone Config** tab.
   If the deactivation failed, the zone configuration still displays in the **Active Zone Config** tab.

6. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Refreshing a zone database

Use this procedure to refresh a zone database.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a zone database from the **Zone DB** list.
4. Select **Refresh** from the **Zone DB Operation** list.

   A message displays informing you that refresh will overwrite the selected database. Click **Yes** to continue.

5. Click **OK**.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Merging two zone databases

If a zone or zone configuration is merged, the resulting zone or zone configuration includes *all* members that were marked for addition or removal as well as all members not otherwise marked.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select **Compare** from the **Zone DB Operation** list.

   The **Compare/Merge Zone DBs** dialog box displays.

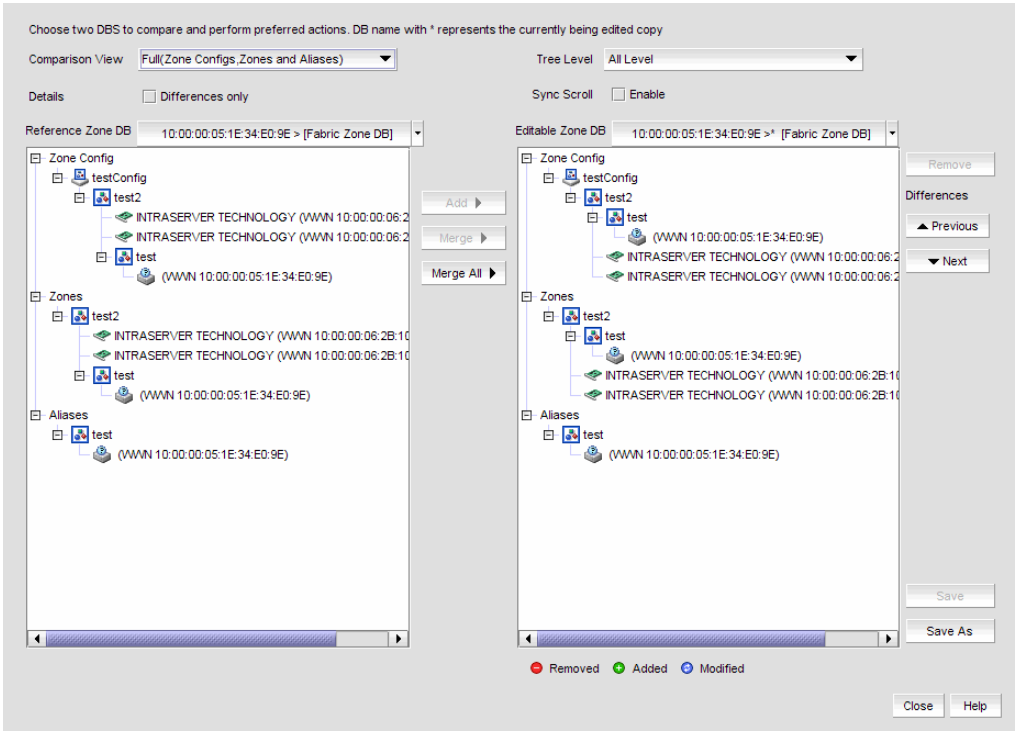


FIGURE 153 Compare/Merge Zone DBs dialog box

3. Select a database from the **Reference Zone DB** field.
4. Select a database from the **Editable Zone DB** field.

   The **Reference Zone DB** and **Editable Zone DB** areas display all available element types (zone configurations, zones, and aliases) for the two selected zone databases. In the **Editable zone DB** area, each element type and element display with an icon indicator (Table 36) to show the differences between the two databases.
5. Set the display for the database areas by selecting one of the following from the **Comparison View** list:
   - **Storage-to-Host Connectivity**—Displays only storage and host devices.
   - **Host-to-Storage Connectivity**—Displays only host and storage devices.
   - **Full (Zone Configs, Zones, Aliases)**—Displays all zone configurations, zones, and aliases.
6. Set the level of detail for the database areas by selecting one of the following options from the **Tree Level** list.

   NOTE
   This list is only available when you set the **Comparison View** to **Full (Zone Configs, Zones, Aliases)**.

   - **All Level**—Displays all zone configurations, zones, and aliases.
   - **Zone Configs**—Displays only zone configurations.
   - **Zones**—Displays only zones.

7. Select the **Differences** check box to display only the differences between the selected databases.
8. Select the **Sync Scroll Enable** check box to synchronize scrolling between the selected databases.
9. Merge zone configurations by completing the followings steps.
    a. Select one or more zone configuration nodes from the **Reference Zone DB** area.
    b. Select an element in the **Editable Zone DB** area.
    c. Click **Merge**.
10. Merge zones by completing the followings steps.
    a. Select one or more zones from the **Reference Zone DB** area.
    b. Select one zone from the **Editable Zone DB** area.
    c. Click **Merge**.
11. Merge aliases by completing the followings steps.
    a. Select one or more aliases from the **Reference Zone DB** area.
    b. Select one alias from the **Editable Zone DB** area.
    c. Click **Merge**.
12. Merge all elements by clicking **Merge All**.
13. Add elements (aliases, zones, and zone configurations) to the editable database by completing the followings steps.
    a. Select one or more of the same elements in the **Reference Zone DB** area.
    b. Select the element type in the **Editable Zone DB** area.
    c. Click **Add**.
14. Remove elements from the editable zone database by selecting an available element (added) from the Editable Zone DB are and clicking **Remove**.

    Note that if a zone is removed from a zone configuration, it is removed *only* from that single zone configuration. However, if the zone is removed from the list of zones, it is removed from *all* zone configurations.

Saving a zone database to a switch

Use this procedure to save a zone database to a switch.

1. Select **Configure > Zoning > Fabric**.

    The **Zoning** dialog box displays.
2. Select a zone database from the **Zone DB** list.
3. Select **Save to Switch** from the **Zone DB Operation** list.

4. Click **Yes** on the confirmation message.

   The selected zone database is saved to the fabric without enabling a specific zone configuration.

5. Click **OK** to save your work and close the **Zoning** dialog box.

Traffic isolation zoning

A Traffic Isolation zone (TI zone) is a special zone that isolates inter-switch traffic to a specific, dedicated path through the fabric. A TI zone contains a list of E_Ports, followed by a list of N_Ports. When the TI zone is activated, the fabric attempts to isolate all inter-switch traffic between N_Ports to only those E_Ports that have been included in the zone. The fabric also attempts to exclude traffic not in the TI zone from using E_Ports within that TI zone.

Traffic isolation zoning is only supported with domain and port index number members.

A TI zone can have failover enabled or disabled.

Disable failover if you want to guarantee that TI zone traffic uses only the dedicated path, and that no other traffic can use the dedicated path.

Enable failover if you want traffic to have alternate routes if either the dedicated or non-dedicated paths cannot be used.

ATTENTION
If failover is disabled, use care when planning your TI zones so that non-TI zone devices are not isolated. If this feature is not used correctly, it can cause major fabric disruptions that are difficult to resolve.

Configuring traffic isolation zoning

The following procedure provides an overview of the steps you must perform to configure traffic isolation zoning.

Note that for any zoning-related procedure, changes to a zone database are not saved until you click **OK** or **Apply** on the **Zoning** dialog box. If you click **Cancel** or the close button (X), no changes are saved.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select **Domain, Port Index** from the **Type** list.
5. If you want to show all discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
6. Create the traffic isolation zones.

   For specific instructions, refer to "Creating a traffic isolation zone" on page 398.

7. Add members to each zone.

   For specific instructions, refer to "Adding members to a traffic isolation zone" on page 399.

   NOTE
   You cannot add a traffic isolation zone to a zone configuration.

8. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas. The traffic isolation zones are activated when you activate a zone configuration in the same zone database.

Creating a traffic isolation zone

Traffic isolation zones are configurable only on a Fabric OS device. The seed switch must be running Fabric OS 6.1.1 or later.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select **Domain, Port Index** from the **Type** list.
5. Select **New TI Zone** from the **New Zone** list.
6. Enter a name for the zone.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 378.

7. Press **Enter**.

   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the zone creation.

8. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Adding members to a traffic isolation zone

NOTE
Traffic isolation zones are only configurable on a Fabric OS device.

Use this procedure to add a member to a zone when the member is listed in the **Potential Members** list of the **Zone DB** tab. Only ports can be added as members to a traffic isolation zone. You must add two or more N_ports as well as all E_ports on the path between the N_ports.

NOTE
You cannot add a device as a member to a traffic isolation zone.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. If you want to show all discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.

5. Select one or more traffic isolation zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)

6. Select **Domain, Port Index** from the **Type** list.

7. Select two or more N_ports (as well as all E_ports on the path between the N_ports) to add to the zone in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each port to select more than one port.)

   NOTE
   TI zones can be created in Fabrics that contain logical switches; however, you can only select physical ports for TI zones.

   If you select a trunk port to add to the TI zone, all trunk ports in the trunk group are added to the TI zone automatically.

8. Click the right arrow between the **Potential Members** list and **Zones** list to add the selected ports to the zone.

   A message may display informing you that one or some of the selected potential members cannot be zoned. Click **OK** to close the message box. Reconsider your selections and make corrections as appropriate.

9. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Enabling a traffic isolation zone

NOTE
Traffic isolation zones are configurable only on a Fabric OS device.

Use this procedure to enable a traffic isolation zone. When a zone configuration in the same zone database is activated, the enabled TI zones are also activated at that time. Traffic isolation zones are enabled by default when you create them.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the traffic isolation zone you want to enable in the **Zones** list and select **Configured Enabled**.
5. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas. The traffic isolation zone is activated when you activate a zone configuration in the same zone database.

Disabling a traffic isolation zone

NOTE
Traffic isolation zones are only configurable on a Fabric OS device.

Traffic isolation zones are enabled by default when you create them. Use this procedure to disable a traffic isolation zone. To apply the settings and deactivate the zone, you must activate a zone configuration in the same zone database.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the traffic isolation zone you want to disable in the **Zones** list and clear the **Configured Enabled** check box.
5. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas. The traffic isolation zone is not disabled until you activate a zone configuration in the same zone database.

Enabling failover on a traffic isolation zone

NOTE
Traffic isolation zones are only configurable on a Fabric OS device.

Use this procedure to enable failover on a traffic isolation zone.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the traffic isolation zone you want to enable failover on in the **Zones** list and select **Configured Failover**.

5. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Disabling failover on a traffic isolation zone

NOTE
Traffic isolation zones are only configurable on a Fabric OS device.

If failover is disabled, be aware of the following considerations:

- Ensure that there are non-dedicated paths through the fabric for all devices that are not in a TI zone.
- If you create a TI zone with just E_Ports, failover must be enabled. If failover is disabled, the specified ISLs will not be able to route any traffic.
- Ensure that there are multiple paths between switches. Disabling failover locks the specified route so that only TI zone traffic can use it.

ATTENTION
If failover is disabled, use care when planning your TI zones so that non-TI zone devices are not isolated. If this feature is not used correctly, it can cause major fabric disruptions that are difficult to resolve.

Use this procedure to disable failover on a traffic isolation zone.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the traffic isolation zone you want to disable failover on in the **Zones** list and clear the **Configured Failover** check box.
5. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Zoning administration

This section provides instructions for performing administrative functions with zoning. You can rename, duplicate, delete, and perform other tasks on zone members, zones, and zone configurations.

Comparing zone databases

You can compare zone databases against one another to identify any and all differences between their membership prior to sending them to the switch. Once the two databases have been compared, icons display to show the differences between the two databases. These icons are illustrated and described in the table below.

TABLE 36 Compare Icon Indicators

Icon	Description
	Added—Displays when an element is added to the editable database.
	Modified—Displays when an element is modified on the editable database.
	Removed—Displays when an element is removed from the editable database.

To compare two zone databases, complete the following steps.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Select **Compare** from the **Zone DB Operation** list.

   The **Compare/Merge Zone DBs** dialog box displays.

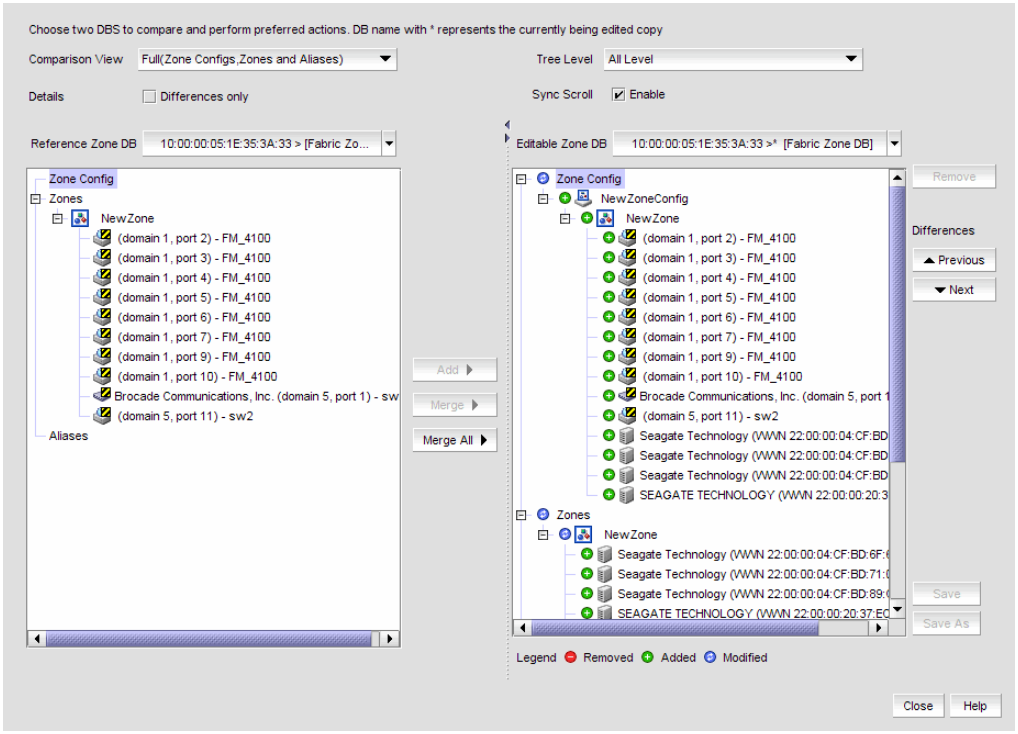


FIGURE 154 Compare/Merge Zone DBs dialog box

3. Select a database from the **Reference Zone DB** field.
4. Select a database from the **Editable Zone DB** field.

   The **Reference Zone DB** and **Editable Zone DB** areas display all available element types (zone configurations, zones, and aliases) for the two selected zone databases. In the **Editable zone DB** area, each element type and element display with an icon indicator (Table 36) to show the differences between the two databases.

5. Set the display for the database areas by selecting one of the following from the **Comparison View** list:

   - **Storage-to-Host Connectivity**—Displays only storage and host devices.
   - **Host-to-Storage Connectivity**—Displays only host and storage devices.
   - **Full (Zone Configs, Zones, Aliases)**—Displays all zone configurations, zones, and aliases.

6. Set the level of detail for the database areas by selecting one of the following options from the **Tree Level** list.

   NOTE
   This list is only available when you set the **Comparison View** to **Full (Zone Configs, Zones, Aliases)**.

   - **All Level**—Displays all zone configurations, zones, and aliases.
   - **Zone Configs**—Displays only zone configurations.
   - **Zones**—Displays only zones.

7. Select the **Differences** check box to display only the differences between the selected databases.

8. Select the **Sync Scroll Enable** check box to synchronize scrolling between the selected databases.
9. Click **Previous** or **Next** to navigate line-by-line in the **Editable Zone DB** area.
10. Click **Close**.

    To merge two zone databases, refer to "Merging two zone databases" on page 394.

Managing zone configuration comparison alerts

You can turn off the automatic zone configuration comparison function if you no longer want to see two of the alert messages that the comparison can produce. When a zone configuration is successfully activated, the comparison function can display an alert icon if either of two conditions exist.

The messages in question are "The active zone configuration does not exist in the zone database" and "The active zone configuration does not match <zone configuration> in the zone database." To turn off the icons and the messages, complete the following steps.

1. After successfully activating a zone configuration, click the **Active Zone Config** tab.
2. Select the check box labeled **Turn off the comparison alerts between the active zone config and the zone database**.

   Any existing alert icons and messages are cleared and further comparisons are prevented.

   The check box selection defaults to the last setting per user.

Setting change limits on zoning activation

Use this procedure to set a limit on the number of changes a user can make to the zone database before activating a zone configuration. If the user exceeds the limit, zone configuration activation is not allowed. Changes include adding, removing, or modifying zones, aliases, and zone configurations.

By default, all fabrics allow unlimited changes.

Using the following procedure you can do the following:

- Set a different limit for each fabric.
- Set limits on some fabrics while allowing other fabrics to have unlimited changes.
- Set a limit for fabrics that will be discovered later.

NOTE
You must have the Zoning Set Edit Limits privilege to perform this task.

1. Select **Configure > Zoning > Set Change Limits**.

   The **Set Change Limits for Zoning Activation** dialog box displays.
2. Click **Change Count** for the fabric on which you want to set limits.

   The field changes to an editable field.

3. Enter the maximum number of zone database changes that can be made for that fabric before a zone configuration is activated.

   To set a limit, enter a positive integer.

   To allow unlimited changes, enter 0.

4. Repeat step 2 and step 3 for each fabric on which you want to set limits.
5. To set a limit for new, undiscovered fabrics, enter a value in the **Default Change Count for New Fabrics** field.

   The default value is 0 (Unlimited).

6. Select the **Enforce change limits during zone activation** check box to enforce the change limits.

   If you want to set the limits now, but turn on enforcement of the limits at a later time, make sure the check box is clear.

7. Click **OK** to save your changes and close the dialog box.

Deleting a zone

Use this procedure to delete a zone.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones in the **Zones** list that you want to delete, then right-click and select **Delete**.

   A message box displays asking you to confirm the deletion.

5. Click **Yes** to delete the selected zone.

   The message box closes and, if successful, the zone or zones are removed from the **Zones** list.

   NOTE
   If you select "**Do not show me this again.**" on the confirmation message box, the next time you delete a zone, the zone is deleted without requesting confirmation from you. If you delete something in error, click **Cancel** on the **Zoning** dialog box to exit without saving changes since the last operation (**Apply** or **Activate**). When you reopen the dialog, the zone is restored.

6. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Deleting a zone alias

Use this procedure to delete a zone alias.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Right-click the zone alias you want to delete and select **Delete.**
5. Click **Yes** on the confirmation message.

   To selected zone alias is deleted from the **Alias** list.

6. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Deleting a zone configuration

Use this procedure to delete a zone configuration.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zone configurations in the **Zone Configs** list that you want to delete, then right-click and select **Delete**.

   A message box displays asking you to confirm the deletion.

5. Click **Yes** to delete the selected zone configuration.

   The message box closes and, when successful, the selected zone configurations are removed from the **Zone Configs** list.

   NOTE
   If you select "**Do not show me this again.**" on the confirmation message box, the next time you delete a zone configuration, it will be deleted without requesting confirmation from you. If you delete something in error, click **Cancel** on the **Zoning** dialog box to exit without saving changes since the last operation (**Apply** or **Activate**). When you reopen the dialog, the zone configuration is restored.

6. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Clearing the fabric zone database

Use this procedure to clear a Fabric Zone database.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning databases for the selected entity.

3. Select the Fabric Zone DB from the **Zone DB** list.

4. Select **Clear All** from the **Zone DB Operation** list.

5. Click **Yes** on the confirmation message.

   The message box closes and, when successful, the Fabric Zone DB is cleared of all zoning configurations.

6. Click **OK** to close the **Zoning** dialog box.

Duplicating a zone

When you duplicate a zone, you make a copy of it in the same zone database. The first time a zone is duplicated, the duplicate is automatically given the name <*zonelabel*>*_copy*. On subsequent times, a sequential number is assigned to the zone name, such as <*zonelabel*>*_copy_1*, <*zonelabel*>*_copy_2,* and <*zonelabel*>*_copy_3*.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones in the **Zones** list that you want to duplicate, then right-click and select **Duplicate**.

   The duplicated zone or zones display in the **Zones** list.

5. Type a new name for the zone, if desired. If not, proceed to Step 5.

   If you key in a new name, press **Enter** to save the name.

   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the renaming. (For zone name requirements and limitations, refer to "Zoning naming conventions" on page 378.)

6. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Duplicating a zone alias

Use this procedure to duplicate a zone alias.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Right-click the zone alias you want to duplicate and select **Duplicate.**

   The duplicated zone alias displays in the **Alias** list (for example, <*Zone_Alias*>_Copy).

5. Edit the name.

   To edit the name, refer to Renaming a zone alias.

6. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Duplicating a zone configuration

When you duplicate a zone configuration, you make a copy of it in the same zone database. The first time a zone configuration is duplicated, the duplicate is automatically given the name <*zonesetlabel*>*_copy*. On subsequent times, a sequential number is assigned to the zone name, such as <*zonesetlabel*>*_copy_1*, <*zonesetlabel*>*_copy_2,* and <*zonesetlabel*>*_copy_3*.

Note that these naming conventions apply both to duplicate and deep duplicate operations.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zone configurations in the **Zone Configs** list that you want to duplicate, then right-click and select one of the following options:

   - **Duplicate** - to duplicate the zone configuration or configurations.
   - **Deep Duplicate** - to duplicate the zone configuration or configurations *and* all included zones.

   The duplicated zone configuration or sets display in the **Zone Configs** list.

5. Type a new name for the zone configuration if desired. If not, proceed to Step 5.

   If you key in a new name, press **Enter** to save the name.

   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the renaming. (For zone configuration name requirements and limitations, refer to "Zoning naming conventions" on page 378.)

6. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Finding a member in one or more zones

Use this procedure to locate all instances of a member in the **Zones** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. If you want to show all fabrics discovered in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.

5. Select the device or port you want to find in the **Potential Members** list.

   Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

6. Click **Find >** between the **Potential Members** list and **Zones** list.

   - If the member is found, all instances of the zone member found are highlighted in the **Zones** list.
   - If the member is not found, a message displays informing you of this. Click **OK** to close the message box.

Finding a zone member in the potential member list

Use this procedure to locate a zone member in the **Potential Members** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone member in the **Zones** list that you want to find in the **Potential Members** list.

   Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

5. Click **Find <** between the **Potential Members list and the Zones** list.

   - If the member is found, it is highlighted in the **Potential Members** list.
   - If the member is not found, a message displays informing you of this. Click **OK** to close the message box.
   - If there are no ports listed in the **Potential Members** list, a message displays informing you that additional action is required. Right-click within the list panel and select **Port Display** from the shortcut menu to display ports.

Finding zones in a zone configuration

Use this procedure to locate all instances of a zone in the **Zone Configs** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone you want to find in the **Zones** list.

   Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

5. Click **Find >** between the **Zones** list and the **Zone Configs** list.

   - If the zone is found, all instances of the zone are highlighted in the **Zone Configs** list.
   - If the zone is not found, a message displays informing you of this. Click **OK** to close the message box.

Finding a zone configuration member in the zones list

Use this procedure to locate a zone configuration member in the **Zones** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone configuration member (i.e., the zone) in the **Zone Configs** list that you want to find in the **Zones** list.

   Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

5. Click **Find <** between the **Zones** list and the **Zone Configs** list.
   - If the zone is found, it is highlighted in the **Zones** list.
   - If the zone is not found, a message displays informing you of this. Click **OK** to close the message box.

Listing zone members

Use this procedure to identify the zone in the active zone configuration of the fabric to which an individual port belongs and the WWN zone members in that zone.

Note that the procedure is performed from the main view of the Management application.

1. On the product device list of the Management application, expand the list of products to show the ports.
2. Select a port and select **Configure > List Zone Members**.

   Keep in mind that only attached device ports can be zoned. If desired, select another port.

   If the port is not a member of a zone, a message displays informing you of this. Click **OK** to close the message.

   If the port is a member of a zone, the **List Zone Members** dialog box displays. The fabric's name, the port's name, and the WWN zone members display.
3. Click **Close** to exit the **List Zone Members** dialog box.

Removing a member from a zone

Use the following procedure to remove one or more members from a zone or zones. Note that the member is not deleted; it is only removed from the zone.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Click the plus sign (+) by the appropriate zone in the **Zones** list to expand the listing and show the zone's members.
5. Perform one of the following actions:
   - Right-click the name of the zone member you want to remove in the **Zones** list and select one of the following options from the shortcut menu that displays:
     - **Remove** - to remove the zone member from the selected zone.
     - **Remove All** - to remove the zone member from all zones to which it belongs.
   - To remove multiple zone members, select the members to be removed from the zone, and click the left arrow between the **Potential Members** list and the **Zones** list.

   When successful, the zone member is removed from the **Zones** list.

6. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Removing a zone from a zone configuration

Use the following procedure to remove a zone from a zone configuration. Note that the zone is not deleted; it is only removed from the zone configuration.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click the plus sign (+) by the appropriate zone configuration in the **Zone Configs** list to expand the listing and show the zone configuration members.

5. Perform one of the following actions:

   - Right-click the name of the zone you want to remove in the **Zone Configs** list and select **Remove**.
   - To remove multiple zones, select the zones to be removed from the zone configuration, and click the left arrow between the **Zones** list and the **Zone Configs** list.

   When successful, the zone is removed from the **Zone Configs** list.

6. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Renaming a zone

Use this procedure to assign a new name to a zone.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the name of the zone you want to change in the **Zones** list and select **Rename**.

5. Type the new name for the zone.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 378.

6. Press **Enter** to save the new name.

   For FC Fabrics, if an invalid name is entered for a zone or zone configuration, the application displays a warning message. If there is a naming violation according to the vendor, the switch returns the error message for the exact information along with the zone configuration activation failure message.

7. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Renaming a zone configuration

Use this procedure to assign a new name to a zone configuration.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the name of the zone configuration you want to change in the **Zone Configs** list and select **Rename**.

5. Type the new name for the zone configuration.

   For zone configuration name requirements and limitations, refer to "Zoning naming conventions" on page 378.

6. Press **Enter** to save the new name.

   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the renaming and consider your options.

7. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Replacing zone members

A zone member can be replaced in a specific, selected zone, or, if it is the member of more than one zone, it can be replaced in all the zones to which it belongs.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the zone member you want to replace in the **Zones** list and select one of the following options from the shortcut menu that displays:

   - **Replace** - to replace the zone member in a selected zone.
   - **Replace All** - to replace all instances of the selected zone member.

   When you select **Replace**, the **Replace Zone Member** dialog box displays. When you select **Replace All**, the same dialog box displays, but with the title **Replace Zone Member (all instances)**.

5. Select the option from the **Type** list that you want to use to identify the replacement zone member.

6. Enter the WWN, name, domain and port index numbers, or alias—whichever is appropriate for the method you chose in step 4.

   When you choose the WWN method, the **Assign Name** field is available; you may define a name for the replacement zone member. If a name was previously assigned to the potential member, a message displays informing you of this and asking whether you want to overwrite the existing name. Click **Yes** to continue and assign a new name, or **No** to decline and dismiss the message box.

7. Click **OK**.

   If you have entered more than one port name or zoning method, a message displays informing you of the error. Click **OK** to close the message, correct your entry, and click **OK** again.

   If no entry error was made, the new zone member replaces the old zone member in the **Zones** list and the **Replace Zone Member** dialog box closes.

8. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Chapter

14

Troubleshooting

In this chapter

- FC troubleshooting 415
- IP troubleshooting 419
- Fabric tracking troubleshooting 424
- Supportsave troubleshooting 424
- Zoning troubleshooting 425

FC troubleshooting

NOTE
FC troubleshooting is only available for Fabric OS devices.

You can perform the following operations using FC troubleshooting:

- Trace Route (Path Information and FC Ping) – Use to obtain the detailed routing information for any two selected device ports. The devices can exist in the same fabric or in two different fabrics shared through FC Routers.
- Device Connectivity Troubleshooting – Use to identify any problems that might be preventing communication between the two selected device ports. The device ports can be selected from the same fabric or from two different fabrics.

Tracing FC routes

The Management application enables you to select a source port and a destination port and displays the detailed routing information from the source port or area on the local switch to the destination port or area on another switch.

Trace route cannot be performed on the offline devices or virtual devices.

NOTE
Trace route is only supported on Fabric OS switches running Fabric OS 5.2 or later.

To trace routes, complete the following steps.

1. Select **Configure > FC Troubleshooting > Trace Route**.

   The **Trace Route** dialog box displays.

2. Choose from one of the following options:

   - Select a fabric from the **Fabric** list.
   - Select a router from the **Routing** list. Requires Fabric OS 6.2 or later.

3. Select the source and destination ports by choosing one of the following:

   The source and destination ports must be on the same fabric; however, they cannot be connected to the same switch.

   - To enter the ports, select the **Enter port FC Address** option.
     a. Enter the source port FC address in the **Source** field.
     f. Enter the destination port FC address in the **Destination** field.
   - To select the ports, select the **Select two device ports** option.
     a. Right-click a fabric in the **Available Device Ports** table and select **Expand All**.
     g. Select the ports (two) for which you want to display the detailed routing information from the **Available Device Ports** table.

4. Click the right arrow button.

5. Click **OK**.

   The **Trace Route Summary** dialog box displays. This dialog box includes the following information:

   - **Trace Route Summary**. This table shows a brief summary of the trace including the port WWN, port name, FC address, switch name, whether ping was successful, round trip time (minimum, maximum, and average) and whether the device ports are in active zones.
   - **Forward Route.** This tab shows the path taken by data packets from the port belonging to the switch on which the trace route has been invoked (source port) to the port on the other switch (destination port).

- **Reverse Route.** This tab shows the path from the destination port to the source port.

  NOTE
  This reverse route may sometimes be different from the forward route.

- **FC Ping.** This tab shows the minimum, maximum and average round trip times between the selected device port WWNs and the domain controller. It details whether the selected device port WWNs are zoned or not. It also shows the number of frames sent to the device port, frames rejected, frames timed-out and frames received by the device port.

6. Click **Close** on the **Trace Route Summary** dialog box.
7. Click **Cancel** on the **Trace Route** dialog box.

Troubleshooting device connectivity

To troubleshoot device connectivity, complete the following steps.

1. Select **Configure > FC Troubleshooting > Device Connectivity**.

   The **Device Connectivity Troubleshooting** dialog box displays.

2. Select the source and destination ports on which you want to troubleshoot device connectivity using one of the following options:

   - Enter the source and destination ports directly by selecting the **Enter port FC Address** option and completing the following steps.

     a. Enter the source port in the **Source** field.

     h. Enter the destination port in the **Destination** field.

     i. Click **Search and Add**.

   - Select the source and destination ports from a list by selecting the **Select two device ports** option and completing the following steps.

     a. Right-click a fabric in the **Available Device Ports** table and select **Expand All**.

     j. Select the ports (source and destination) for which you want to confirm device sharing from the **Available Device Ports** table.
     To add a detached device to troubleshoot device connectivity, refer to "Adding detached device" on page 418.

     k. Click the right arrow button.

3. Click **OK**.

   The following diagnostic tests are performed:

   - Device Status
   - Switch port health status
   - Zone configuration in the fabric
   - Edge fabric - FC router physical connection status.
   - Active ACL DCC policy check (Fabric OS only)

   The **Device Connectivity Troubleshooting Results** dialog box displays.

   If no problems are found, the diagnostic test is marked with a check mark. If problems are found, an alert icon appears next to the test, with a brief statement detailing the error as well as a suggested resolution.

4. Click **Re-run Diagnosis** to run the device connectivity on the same ports.
5. Click **Trace Route** to trace the route between the two selected ports.
6. Click **Close** on the **Device Connectivity Troubleshooting Results** dialog box.

Adding detached device

To add a detached device to the **Selected Device Ports** table, complete the following steps.

1. Click Add Detached from the **Device Connectivity Troubleshooting** dialog box.
2. Add the detached device port by choosing one of the following:
   - To add by port WWN, select the **By Port WWN** option.
   - To add by FC address, select the **By FC Address** option.
3. Enter the port WWN or FC address in the field.
4. Click **OK**.

IP troubleshooting

NOTE
IP troubleshooting is only available for Fabric OS devices.

You can perform the following operations using IP troubleshooting:

- **Ping.** Use to confirm that the configured FCIP tunnels are working correctly.
- **Trace Route.** Use to view the route information from a source port on the local device to a destination port on another device and determine where connectivity is broken.
- **Performance.** Select to view FCIP tunnel performance between two devices.

Configuring IP ping

NOTE
IP Ping only supported on Fabric OS devices running Fabric OS 5.2 or later.

To configure IP ping, complete the following steps.

1. Select **Configure > IP Troubleshooting > Ping**.

   The **IP Ping** dialog box displays.

2. Select a switch from the **Available Switches** table.
3. Select a port from the **GigE Port** list.
4. Select an IP address switch from the **IP Interface** list.
5. Enter the remote IP address in the **Remote IP Address** field.
6. Click **OK**.

   Ping sends four Internet Control Message Protocol (ICMP) Ping packets to the destination address and records the time until a response.

   The **IP Ping Result** dialog box displays with two tables.

   The top table (**FCIP IP Ping Response Details**) contains the following statistics:

TABLE 37 FCIP IP Ping Response Details

Field or Component	Description
Status	Always displays 'Completed'. If there is a failure, an error message displays instead of the **IP Ping Result** dialog box.
Packets Sent	Always displays '4. This is not configurable.
Packets Received	The number of received responses.
Packets Lost	Equal to the number of packets sent minus the number of packets received.
Packet Lost percentage	The number of packets lost expressed as a percentage of the packets sent. This will be 0%, 25%, 50%, 75% or 100% for 0, 1, 2, 3, or all 4 packets lost.
Minimum Round Trip Time	The shortest time, in milliseconds, of any response. If no response, the round trip times is 0.

TABLE 37 FCIP IP Ping Response Details

Field or Component	Description
Maximum Round Trip Time	The longest time, in milliseconds, of any response. If no response, the round trip times is 0.
Average Round Trip Time	The average time, in milliseconds, of all responses. If no response, the round trip times is 0.

The bottom table (**IP Ping Details**) provides details for each ping attempt.

TABLE 38 IP Ping Details

Field or Component	Description
Reply From	The IP address of the device that sent the reply. For a normal response, this is the destination IP address. Some error responses (such as "destination unreachable") may come from an intermediate router.
Status	Displays either Success or an error message (such as request timed out or destination unreachable) from the switch.
Number of bytes	The number of bytes in the data portion of the response. Should be 64, matching the 64 bytes of data sent in the transmitted packet.
Round Trip Time (ms)	The time in milliseconds between sending the packet and receiving the response. This provides a rough indication of network congestion or latency. It is normal for the first packet to experience a higher round trip time than later packets, if the intermediate routers need to do ARP requests to locate the next hop.
Time To Live (hops)	The number of hops remaining in the received response. The time to live is decremented by each router that forwards the packet. The packet is dropped if the time to live reaches zero.

7. Click **Close** on the **IP Ping Result** dialog box.
8. Click **Cancel** on the **IP Ping** dialog box.

Tracing IP routes

The Management application enables you to select an source and a target and displays the detailed routing information from the source port or area on the local switch to the destination port or area on another switch.

Trace route cannot be performed on the offline devices or virtual devices.

NOTE
Trace route is only supported on Fabric OS devices running Fabric OS 5.2 or later.

To trace routes, complete the following steps.

1. Select **Configure > IP Troubleshooting > Trace Route**.

   The **IP Traceroute** dialog box displays.

2. Select a switch from the **Available Switches** table.
3. Select a port from the **GigE Port** list.
4. Select an IP address switch from the **IP Interface** list.
5. Enter the remote IP address in the **Remote IP Address** field.
6. Click **OK**.

   The **IP Traceroute Result** dialog box displays.

   Traceroute sends three ICMP Ping packets to the destination address with a time to live (TTL) of one hop, and expects a 'TTL Expired' error back from the first router to obtain the IP address of the first hop. Traceroute then repeats the operation with a TTL of two hops to get the IP address of the second hop. This process repeats for up to ten hops, or until a successful PING response is received.

   The IP Trace Details table displays the results of each attempt.

TABLE 39 IP Trace Details

Field or Component	Description
Hop Number	The TTL inserted in the transmitted probe packet.
IP Address 1	The IP address of the system that responded to the first of the three probes, or 0.0.0.0 if there was no response.
IP Address 2	The IP address of the system that responded to the second of the three probes, or 0.0.0.0 if there was no response.
IP Address 3	The IP address of the system that responded to the third of the three probes, or 0.0.0.0 if there was no response.
RTT 1	The time in milliseconds for the first of the three responses to be received, or blank if there was no response. This value helps identify a congested or slow link in the path.
RTT 2	the time in milliseconds for the second of the three responses to be received, or blank if there was no response. This value helps identify a congested or slow link in the path.
RTT 3	the time in milliseconds for the third of the three responses to be received, or blank if there was no response. This value helps identify a congested or slow link in the path.

7. Click **Close** on the **IP Traceroute Result** dialog box.
8. Click **Cancel** on the **IP Traceroute** dialog box.

Viewing FCIP tunnel performance

NOTE
IP Performance is only supported on the 4 Gbps Router, Extension Switch and Encryption Blade running Fabric OS 5.2 or later.

NOTE
If you run IP Performance over a link also being used for production traffic, it will impact the production traffic performance.

To view FCIP tunnel performance, complete the following steps.

1. Select **Configure > IP Troubleshooting > Performance**.

   The **IP Performance** dialog box displays.
2. Select a switch from the **Available Switches** table.
3. Select a port from the **GigE Port** list.
4. Select an IP address switch from the **IP Interface** list.
5. Enter the remote IP address in the **Remote IP Address** field.
6. Click **OK**.

   The **IP Performance Result** dialog box displays.

   IP Performance sends dummy data as fast as possible to the remote IP address and measures how much data can be sent over a given interval. IP Performance attempts to saturate the network link to see how much bandwidth is available. It will display the media link bandwidth only if no other traffic is flowing. The remote IP address must belong to a managed switch so that IP Performance can set up the receiving end on the remote switch.

   For more information about IP Performance, refer to Chapter 20 in the *Fabric OS Administrator's Guide*.

   During the IP Performance test, data is sent continuously and statistics are sampled every 30 seconds. At the end of the period, the IP Performance results dialog is displayed. The IP Performance results dialog contains a table with one row for each 30-second sample of the test. Columns in the perf results dialog are:

TABLE 40

Field/Component	Description
Available Bandwidth	The average bytes per second sent during the sample interval. This is a count of FC payload bytes; for example, the throughput seen by an FC application. It is slightly lower than the actual bytes-per-second on the wire since it does not include headers and acknowledgements.
Weighted Bandwidth	The weighted bandwidth represents what the FCIP tunnel / FC application sees for throughput rather than the Ethernet on-the-wire bytes.
Loss Percent	An estimate of the percentage of data packets lost during the sampling interval, based on TCP re-transmits.

TABLE 40

Field/Component	Description
DELAY	The average round trip time to send a packet of data and receive the acknowledgement.
PMTU (Path Maximum Transmission Unit)	The largest packet size that can be transmitted over the end-to- end path without fragmentation. This value is measured in bytes and includes the IP header and payload. IP Performance tries the configured Fabric OS Jumbo MTU value (anything over 15000, then 1500, then 1260. The value displayed in the table is the largest value that worked.

7. Click **Close** on the **IP Performance Result** dialog box.
8. Click **Cancel** on the **IP Performance** dialog box.

Client browser troubleshooting

The following section states a possible issue and the recommended solution for client browser errors.

TABLE 41 Client browser issues

Problem	Resolution
Downloading Client from a Internet Explorer Browser over HTTPS	If the JNLP file does not launch automatically, use one of the following options: • Complete the following steps. 1 Save the JNLP file to the local host. 2 Launch the JNLP file manually. • In Internet Explorer 7, complete the following steps. 1 Select **Tools > Internet Options**. 2 Click the **Advanced** tab. 3 Clear the **Do not save encrypted pages to disk** check box. If the browser warns you about the security certificate, use the fully qualified hostname to launch the web page.

Fabric tracking troubleshooting

The following section states a possible issue and the recommended solution for fabric tracking errors.

TABLE 42 Fabric tracking issues

Problem	Resolution
If a switch is replaced by another switch having the same IP address but a different node WWN while fabric tracking is on, the Management application does not update the Product List, Connectivity Map or switch properties with the new node WWN.	Choose from one of the following options: • Turn fabric tracking off while the switch is replaced. This causes the old switch to be removed and the new switch added. • After the switch is replaced, remove and re-add the fabric in the **Discover Setup** dialog box.

Professional edition login troubleshooting

The following section states a possible issue and the recommended solution for Professional edition login errors.

TABLE 43 Professional edition login issues

Problem	Resolution
Login Failed. Only one client allowed. One client session is active or has not yet timed out.	If you closed the client using Windows Task Manager (End Task or Process) or using Linux or Solaris process ID (kill command), successful relaunch of the application may take up to 2 minutes.

Supportsave troubleshooting

The following section states a possible issue and the recommended solution for supportsave errors.

TABLE 44 Supportsave issues

Problem	Resolution
Cannot capture support save information.	Capture support show by running the batch file from the *<Install_Home>*/bin/supportshow.bat from Windows and UNIX systems. 1 *Open <Install_Home>*\bin\supportsave.bat. 2 Edit file `supportsave dbuser dbpasswd [tareget-dir] [pause-option]`.

Zoning troubleshooting

The following section states some possible issues and recommended solutions for zoning errors.

TABLE 45 Zoning issues

Problem	Resolution
Cannot perform zoning on a new switch.	You must use telnet (or the *Product Type and Access* tab in the *Add Properties* dialog box) to change the default password on the new switch before you can use the Management application to perform zoning.
When configuring a large zone configuration a switch displays offline during discovery.	If a large zone configuration is configured in a fabric, switches may temporarily display as being offline during discovery. Wait for the next discovery cycle and click the *Refresh* button on the toolbar.
When activating a large zone configuration on a two-switch fabric on UNIX platforms, an error message displays stating “Failed to perform the requested zoning action: Failed to zone due to exception.”	Although the error message states that the requested zoning action failed, the zone configuration will be correctly activated. Wait for the next zoning polling to occur. This issue only occurs on UNIX systems.
Zoning activation message displays for a long time, but zone configuration is not activated.	Telnet zoning can take a long time. To improve speed, open the *Discover > Setup* dialog box and add the IP address for the device to the *Selected Individual Addresses* list.

Appendix

Supported Key Management Systems

A

In this appendix

- Key management systems 427
- The NetApp Lifetime Key Manager 428
- The RSA Key Manager 436
- The HP Secure Key Manager 440
- Thales Encryption Manager for Storage 451

Key management systems

Data is encrypted and decrypted using the same Data encryption key (DEK), so a DEK must be preserved at least long enough to decrypt the ciphertext that was created using that DEK. The length of time data is stored before it is retrieved can vary greatly. Some data may be stored for months, years or decades before it is accessed. To be sure encrypted data remains accessible DEKs also need to be stored for months, years or decades. This requires the use of a key management system.

Key management systems are available from several vendors to provide life cycle management for all DEKs created by the encryption engine. The following key management systems currently support Brocade encryption switches and blades:

- NetApp Lifetime Key Manager (LKM).
- RSA Key Manager (RKM).
- Hewlett Packard Secure Key Manager (HP SKM).
- Thales Encryption Manager for Storage (TEMS), also referred to as the nCipher Key Authority (NCKA) within operational descriptions in this document.

.

The NetApp Lifetime Key Manager

The NetApp Lifetime Key Manager (LKM) resides on an FIPS 140-2 Level 3-compliant network appliance. The encryption engine and LKM appliance communicate over a trusted link. A trusted link is a secure connection established between the Encryption switch or blade and the NetApp LKM appliance, using a shared secret called a link key. One link key per encryption switch is established with each LKM appliance. On a Brocade DCX or DCX-4S or with one or two FS8-18 encryption blades, only one link key is established with each LKM appliance, and the link key is shared between the blades.

DEKs are encrypted by the encryption engine, using its link key, and passed to LKM over a secure connection. LKM decrypts the DEKs and encrypts them on the LKM appliance. When the encryption engine needs a DEK from the LKM key vault, it passes a request that includes a key ID and other parameters needed by LKM to locate the correct key. LKM locates the DEK, decrypts it, and then encrypts it using the its key for transfer to the encryption engine.

Setting up an LKM key vault consists of the following steps:

- Authenticating the NetApp LKM appliance with the group leader by registering certificates containing the public key and IP address with the group leader. The group leader automatically distributes the certificate and the IP address of the NetApp LKM appliance to all group members.
- Authenticating the encryption group leader and each encryption group member with the NetApp LKM appliance. For each node in the encryption group, the IP address and the certificate containing the public key are registered with the NetApp LKM appliance. The registered certificate is a special purpose KAC Certificate that contains license information related to the LKM.
- Establishing a trusted link between the NetApp LKM appliance and each member node. As part of the trusted link establishment, a shared secret called a link key is created on each of the two entities, The link key is subsequently used for encrypting the DEKs for archival to the NetApp LKM appliance or for decrypting the encrypted DEKs for retrieval from the NetApp LKM appliance.

The NetApp DataFort Management Console

The NetApp DataFort Management Console (DMC) must be installed on your PC or workstation to complete certain procedures described in this appendix. Refer to the appropriate DMC product documentation for DMC installation instructions. After you install DMC, do the following.

1. Launch the DMC.
2. Click the **Appliance** tab on the top panel.
3. Add the NetApp LKM appliance IP address or hostname.
4. Right-click the added IP address and log into the NetApp LKM key vault.

Obtaining and importing the LKM certificate

Certificates must be exchanged between LKM and the encryption switch to enable mutual authentication. You must obtain a certificate from LKM, and import it into the encryption group leader. The encryption group leader exports the certificate to other encryption group members.

To obtain and import an LKM certificate, do the following.

1. Open an SSH connection to the NetApp LKM appliance and log in.

```
host$ssh admin@10.33.54.231
admin@10.33.54.231's password:

Copyright (c) 2001-2009 NetApp, Inc.
All rights reserved
+-------------------------------+
| NetApp Appliance Management CLI |
|      Authorized use only!      |
+-------------------------------+
Cannot read termcapdatabase;
using dumb terminal settings.
Checking system tamper status:
No physical intrusion detected.
```

2. Add the group leader to the LKM key sharing group. Enter **lkmserver add --type third-party --key-sharing-group "/"** followed by the group leader IP address.

```
lkm-1>lkmserver add --type third-party --key-sharing-group \
   "/" 10.32.244.71
NOTICE: LKM Server third-party 10.32.244.71 added.
Cleartext connections not allowed.
```

3. On the NetApp LKM appliance terminal, enter **sys cert getcert-v2** to display the LKM certificate content.

```
lkm-1> sys cert getcert-v2
-----BEGIN CERTIFICATE-----
[content removed]
-----END CERTIFICATE-----
```

4. Copy and paste the LKM certificate content from the NetApp LKM appliance terminal into an editor buffer. Save the file as **lkmcert.pem** on the SCP-capable host. Save the entire certificate, including the lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.

5. On the group leader, import the previously saved LKM certificate from the SCP-capable host:

   - If you are using the Management application, the path to the file must be specified on the **Select Key Vault** dialog box. If the proper path is entered, the file is imported.
   - If you are using the CLI, use the **cryptocfg – import** command with the **-scp** option. The following example imports a certificate file named lkmcert.pem.

```
SecurityAdmin:switch>cryptocfg --import -scp lkmcert.pem 192.168.38.245 \
                     mylogin /tmp/certs/lkmcert.pem
Password:
Operation succeeded.
```

Exporting the KAC certificate signing request

If you are using the SAN Management program, the KAC certificate signing request (CSR) is exported to a location you specify when you create a new encryption group or add a switch to an encryption group. You can also export the KAC CSR from the **Switch Properties** view.

If you are using the CLI, you can export the KAC CSR from the switch to a file on a LAN-attached host, or you can attach a USB storage device to the switch and export the KAC CSR to that device.

1. Log into the switch on which the CSR was generated as Admin or SecurityAdmin.
2. Export the CSR from the switch over an SCP-protected LAN connection to a file on an external host (e.g., your workstation), or to a mounted USB device.

   The following example exports a CSR to an external SCP-capable host.

   ```
   SecurityAdmin:switch>cryptocfg --export -scp -KACcsr \
   192.168.38.245 mylogin /tmp/certs/kac_lkm_cert.pem
   Password:
   Operation succeeded.
   ```

   The following example exports a CSR to USB storage.

   ```
   SecurityAdmin:switch>cryptocfg --export -usb KACcsr kac_lkm_cert.pem
   Operation succeeded.
   ```

   If you export the CSR to a USB storage device, you will need to remove the storage device from the switch, and attached it to a computer that has access to a third party certificate authority (CA). If you are using the SAN Management program, this can be your SAN Management program workstation. The CSR must be submitted to a CA.

NOTE
The CSR is exported in Privacy Enhanced Mail (.pem) format. This format is required in exchanges with certificate authorities.

Submitting the CSR to a certificate authority

The CSR must be submitted to a certificate authority (CA) to be signed. The certificate authority is a trusted third party entity that signs the CSR. There are several CAs available, and procedures vary, but the general steps are as follows.

1. Open an SSL connection to an X.509 server.
2. Submit the CSR for signing.
3. Request the signed certificate.

   Generally, a public key, the signed KAC certificate, and a signed CA certificate are returned.
4. Store the signed certificates, preferably in the same location as the CSR.

Importing the signed KAC certificate

The signed KAC certificate must be imported into the switch or blade that generated the CSR.

If you are using the SAN Management program, do the following.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays the status of all encryption-related hardware and functions at a glance. It is the single launching point for all encryption-related configuration.

2. Select the switch or encryption engine from the **Encryption Devices** table, and select **Switch > Properties** or **Engine > Properties** from the menu bar, or right-click the switch or encryption engine and select **Properties**.

   The **Encryption Properties** dialog box is displayed.

3. Click **Import**

   An **Open** dialog box is displayed.

4. From **Look In**, browse to the location where you stored the signed KAC certificate after you received it from the CA.

5. To limit the number of files displayed to .pem files, select Certificate Files (*.pem) from **Files of Type**.

6. Select the file and click **Open**.

   You are returned to **Encryption Properties**.

7. Click **Save**.

If you are using the CLI, you can import the signed KAC certificate to the switch from a file on a LAN-attached host, or you can write it to a USB storage device, attach the USB storage device to the switch or blade, and import the certificate from that device. The following describes both options.

1. Log into the switch to which you wish to import the certificate as Admin or SecurityAdmin.

2. Enter the **cryptocfg --import** command with the appropriate parameters.

   The following example imports a CP certificate named “enc_switch1_cp_cert.pem” that was previously exported to the external host 192.168.38.245. Certificates are imported to a predetermined directory on the node.

   ```
   SecurityAdmin:swicth>cryptocfg --import -scp enc_switch1_cp_cert.pem \
   192.168.38.245 mylogin /tmp/certs/enc_switch1_cp_cert.pem
   Password:
   Operation succeeded.
   ```

   The following example imports a CP certificate named “enc_switch1_cp_cert.pem” that was previously exported to USB storage.

   ```
   SecurityAdmin:switch>cryptocfg --import -usb enc_switch1_cp_cert.pem \
   enc_switch1_cp_cert.pem
   Operation succeeded.
   ```

Registering the certificates

The switch's KAC certificate must be registered on the LKM appliance, and the LKM certificate must be registered on the switch.

1. From the external host, register the KAC certificate you exported from the group leader with the NetApp LKM appliance.

```
host$echo lkmserver certificate set 10.32.244.71 \
'cat kac_lkm_cert.pem' | ssh -l admin 10.33.54.231
Pseudo-terminal will not be allocated because stdinis not a terminal.
admin@10.33.54.231's password:
Checking system tamper status:
No physical intrusion detected.
NOTICE: LKM Peer '10.32.244.71' certificate is set
```

2. On the group leader, register the NetApp LKM appliance as the primary key vault LKM1.

```
SecurityAdmin:switch>cryptocfg --reg -keyvault LKM1 lkmcert.pem \
10.33.54.231 primary
lkm-1
Register key vault status: Operation Succeeded.
```

3. Display the registered key vault on the group leader. The LKM key vault is shown as connected.

```
SecurityAdmin:switch>cryptocfg --show -groupcfg
Encryption Group Name:       brocade
  Failback mode:             Manual
  Heartbeat misses:          3
  Heartbeat timeout:         2
  Key Vault Type:            LKM
Primary Key Vault:
  IP address:                10.33.54.231
  Certificate ID:            lkm-1
  Certificate label:         LKM1
  State:                     Connected
  Type: LKM
Secondary Key Vault not configured
NODE LIST
Total Number of defined nodes:   2
Group Leader Node Name:          10:00:00:05:1e:41:7e
Encryption Group state:          CLUSTER_STATE_CONVERGED
Node Name               IP address      Role
10:00:00:05:1e:41:9a:7e  10.32.244.71  GroupLeader(current node)
10:00:00:05:1e:39:14:00  10.32.244.60  MemberNode
```

4. Display the registered key vault on the member node. The LKM key vault is shown as not responding because certificates have not been exchanged.

```
SecurityAdmin:enc1_switch>cryptocfg --show -groupcfg
Encryption Group Name:          brocade
  Failback mode:                Manual
  Heartbeat misses:          3
  Heartbeat timeout:         2
  Key Vault Type:            LKM
Primary Key Vault:
  IP address:                10.33.54.231
  Certificate ID:            lkm-1
  Certificate label:         LKM1
  State:                     Not responding
  Type: LKM
Secondary Key Vault not configured
```

```
NODE LIST
Total Number of defined nodes: 2
Group Leader Node Name:        10:00:00:05:1e:41:7e
Encryption Group state:        CLUSTER_STATE_CONVERGED
Node Name               IP address      Role
10:00:00:05:1e:41:9a:7e  10.32.244.71  GroupLeader
10:00:00:05:1e:39:14:00  10.32.244.60  MemberNode (current node)
```

5. Exchange certificates between the LKM key vault and the member node, starting with exporting the KAC certificate from the member node to an SCP-capable external host.

```
SecurityAdmin:enc1_switch>cryptocfg --export -scp -KACcert \
192.168.38.245 mylogin enc1_kac_lkm_cert.pem
Password:
Operation succeeded.
```

6. Open an SSH connection to the NetApp LKM appliance and add the member node IP address.

```
lkm-1> lkmserver add --type third-party --key-sharing-group "/" \
10.32.244.60
NOTICE: LKM Server third-party 10.32.244.60 added.
Cleartext connections not allowed.
```

7. On the external host, register the KAC LKM certificate you exported from the member node with the NetApp LKM appliance.

```
host$echo lkmserver certificate set 10.32.244.60
'cat enc1_kac_lkm_cert.pem' | ssh-l admin 10.33.54.231
Pseudo-terminal will not be allocated because stdinis not a terminal.
admin@10.33.54.231's password:
Checking system tamper status:No physical intrusion detected.
ALERT: There are pending unapproved trustees.
NOTICE: LKM Peer '10.32.244.60' certificate is set
```

8. Enter the **cryptocfg --show -groupcfg** command on the member node. If the link key has been established (refer to "Establishing the trusted link"), the display shows the LKM as connected.

```
SecurityAdmin:enc1_switch>cryptocfg --show -groupcfg
Encryption Group Name:       brocade
  Failback mode:             Manual
  Heartbeat misses:          3
  Heartbeat timeout:         2
  Key Vault Type:            LKM
Primary Key Vault:
  IP address:                10.33.54.231
  Certificate ID:            lkm-1
  Certificate label:         LKM1
  State:                     Connected
  Type: LKM
Secondary Key Vault not configured
[output truncated]
```

LKM appliance cluster support

LKM appliances can be clustered together to provide high availability (HA) failover/failback capabilities. When LKM appliances are clustered, both LKMs in the cluster must be registered and configured with the link keys before starting any crypto operations. If two LKM key vaults are configured, they must be clustered. If only a single LKM key vault is configured, it may be clustered for backup purposes, but it will not be directly used by the switch.

The following rules apply to key archival and retrieval operations in an HA key vault deployment scenario:

- For key archival operations:
  - Before the LKM key is used for cryptographic operations, the key is archived to both key vaults (primary and secondary). If either of them is not available, Key archival operations will fail.
  - If key archival fails because of key vault failure, an ERROR is logged.
- For key retrieval operations:
  - Key retrieval operations are requested from either the primary or secondary LKM, whichever is operational and reachable from the encryption switch or blade.

In the event of a fatal key vault error, replace the failed LKM and link the replacement LKM to the existing LKM. Refer to the LKM product documentation for further information on replacing a failed LKM.

Establishing the trusted link

You must generate the trusted link establishment package (TEP) on all nodes to obtain a trusted acceptance package (TAP) before you can establish a trusted link between each node and the NetApp LKM appliance. You must have a card reader attached to your PC or workstation to complete the procedure.

NOTE
Complete all steps required to establish a trusted link between LKM and the encryption group members for each node before proceeding to the next node.

1. Open an SSH connection to the NetApp LKM appliance and log in.

```
host$ssh admin@10.33.54.231
admin@10.33.54.231's password:

Copyright (c) 2001-2008 NetApp, Inc.
All rights reserved
+-------------------------------+
| NetApp Appliance Management CLI |
|      Authorized use only!      |
+-------------------------------+
Cannot read termcapdatabase;
using dumb terminal settings.
Checking system tamper status:
No physical intrusion detected.
```

2. To add the encryption group leader to an LKM appliance third party key sharing group, enter **lkmserver add --type third-party --key-sharing-group "/"** followed by the group leader IP address.

```
lkm-1>lkmserver add --type third-party --key-sharing-group \
   "/" 10.32.244.71
NOTICE: LKM Server third-party 10.32.244.71 added.
Cleartext connections not allowed.
```

3. From the external host, enter **echo lkmserver set <group leader IP address> 'cat kac_cert_lkm.pem' | ssh -l admin <LKM IP address>** to register the KAC LKM certificate you exported from the group leader with the NetApp LKM appliance.

```
host$echo lkmserver certificate set 10.32.244.71 \
'cat kac_lkm_cert.pem' | ssh -l admin 10.33.54.231
Pseudo-terminal will not be allocated because stdinis not a terminal.
admin@10.33.54.231's password:
Checking system tamper status:
No physical intrusion detected.
NOTICE: LKM Peer '10.32.244.71' certificate is set
```

4. Select the **Link Keys** tab on the **Encryption Group Properties** dialog box.

   The switch name displays in the link status table under **Switch**, with a **Link Key Status** of **Link Key requested, pending LKM approval**.

5. Select the switch, and click **Establish**.

   This results in a Trusted link establishment package (TEP), which is needed to establish the trusted link between the switch and the LKM appliance.

6. Launch the NetApp DataFort Management Console (DMC) and click the **View Unapproved Trustees** tab.

   The switch is listed as openkey_trustee_<ip address>, where the IP address is the switch IP address entered in step 2.

7. Select the switch, and click **Approve and Create TAP**.

   The **Approve TEP** dialog box displays. The TEP must be approved before a TAP can be created.

8. Provide a label in the dialog box and click **Approve** to approve the TEP.

   A list of recovery cards and recovery officers is displayed. TEP approval is done by a quorum of recovery officers, using assigned recovery cards. Each recovery officer must individually insert one of listed recovery cards into a card reader attached to the PC or workstation, enter the password for that card, and click **Start**. The procedure is repeated until a quorum of recovery officers has approved the TEP.

9. Save the TAP to a file (location does not matter).

10. Select the **Link Keys** tab on the **Encryption Group Properties** dialog box.

11. Select the switch in the link key status table, and click **Accept** to retrieve the TAP from the LKM appliance.

12. Repeat the above steps for the each of the remaining member nodes.

The RSA Key Manager

Communication with the RSA Key Manager (RKM) is secured by wrapping DEKs in a master key. The encryption engine must generate its own master key, send DEKs to RKM encrypted in the master key, and decrypt DEKs received from RKM using the same master key. The master key may optionally be stored as a key record in the RKM key vault as a backup, but RKM does not assume responsibility for the master key. The master key must be backed up and stored, and policies and procedures for responding to theft or loss must be in place.

Obtaining and Importing the RKM certificate

Certificates must be exchanged between RKM and the encryption switch to enable mutual authentication. You must obtain a certificate from RKM, and import it into the encryption group leader. The encryption group leader exports the certificate to other encryption group members.

To obtain and import an RKM certificate, do the following.

1. Export the RKM certificate using a file transfer utility, such as FTP, and save it on an SCP-capable host.
2. On the group leader, import the previously saved RKM certificate from the SCP-capable host:
   - If you are using the Management application, the path to the file must be specified on the **Select Key Vault** dialog box. If the proper path is entered, the file is imported.
   - If you are using the CLI, use the **cryptocfg – import** command with the **-scp** option. The following example imports a certificate file named rkmcert.pem.

     ```
     SecurityAdmin:switch>cryptocfg --import -scp rkmcert.pem 192.168.38.245 \
                          mylogin /tmp/certs/rkmcert.pem
     Password:
     Operation succeeded.
     ```

Exporting the KAC certificate signing request (CSR)

If you are using the SAN Management program, the KAC CSR is exported to a location you specify when you create a new encryption group or add a switch to an encryption group. If you are using the CLI, you can export the KAC CSR from the switch to file on a LAN-attached host, or you can attach a USB storage device to the switch and export the KAC CSR to that device.

1. Log into the switch on which the CSR was generated as Admin or SecurityAdmin.
2. Export the CSR from the switch over an SCP-protected LAN connection to a file on an external host (e.g., your workstation), or to a mounted USB device.

   The following example exports a CSR to an external SCP-capable host.

   ```
   SecurityAdmin:switch>cryptocfg --export -scp -KACcsr \
   192.168.38.245 mylogin /tmp/certs/kac_rkm_cert.pem
   Password:
   Operation succeeded.
   ```

The following example exports a CSR to USB storage.

```
SecurityAdmin:switch>cryptocfg --export -usb KACcsr kac_rkm_cert.pem
Operation succeeded.
```

If you export the CSR to a USB storage device, you will need to remove the storage device from the switch, and then attach it to a computer that has access to a third party certificate authority (CA). If you are using the SAN Management application, this can be your SAN Management application workstation. The CSR must be submitted to a CA.

NOTE
The CSR is exported in Privacy Enhanced Mail (.pem) format. The is the format required in exchanges with certificate authorities.

Submitting the CSR to a certificate authority

The CSR must be submitted to a certificate authority (CA) to be signed. The certificate authority is a trusted third party entity that signs the CSR. There are several CAs available, and procedures vary, but the general steps are as follows.

1. Open an SSL connection to an X.509 server.
2. Submit the CSR for signing.
3. Request the signed certificate.

   Generally, a public key, the signed KAC certificate, and a signed CA certificate are returned.
4. Store the signed certificates, preferably in the same location as the CSR.

Importing the signed KAC certificate

The signed KAC certificate must be imported into the switch or blade that generated the CSR.

If you are using the SAN Management program, do the following.

1. Select **Configure > Encryption** from the menu bar.

   The **Encryption Center** dialog box displays the status of all encryption-related hardware and functions at a glance. It is the single launching point for all encryption-related configuration.
2. Select the switch or encryption engine from the **Encryption Devices** table, and select **Switch > Properties** or **Engine > Properties** from the menu bar, or right-click the switch or encryption engine and select **Properties**.

   The **Encryption Properties** dialog box is displayed.
3. Click **Import**

   An **Open** dialog box is displayed.
4. From **Look In**, browse to the location where you stored the signed KAC certificate after you received it from the CA.
5. To limit the number of files displayed to .pem files, select Certificate Files (*.pem) from **Files of Type**.
6. Select the file and click **Open**.

   You are returned to **Encryption Properties**.

7. Click **Save**.

If you are using the CLI, you can import the signed KAC certificate to the switch from a file on a LAN attached host, or you can write it to a USB storage device, attach the USB storage device to the switch or blade, and import the certificate from that device. The following describes both options.

1. Log into the switch to which you wish to import the certificate as Admin or SecurityAdmin.
2. Enter the **cryptocfg --import** command with the appropriate parameters.

   The following example imports a CP certificate named “enc_switch1_cp_cert.pem” that was previously exported to the external host 192.168.38.245. Certificates are imported to a predetermined directory on the node.

   ```
   SecurityAdmin:switch>cryptocfg --import -scp enc_switch1_cp_cert.pem \
   192.168.38.245 mylogin /tmp/certs/enc_switch1_cp_cert.pem
   Password:
   Operation succeeded.
   ```

   The following example imports a CP certificate named “enc_switch1_cp_cert.pem” that was previously exported to USB storage.

   ```
   SecurityAdmin:switch>cryptocfg --import -usb enc_switch1_cp_cert.pem \
   enc_switch1_cp_cert.pem
   Operation succeeded.
   ```

3. Register the KAC certificate.

   ```
   SecurityAdmin:switch>cryptocfg --reg -KACcert <certificate file>
   ```

Uploading the KAC and CA certificates onto the RKM appliance

After an encryption group is created, you need to install the switch public key certificate (KAC certificate) and signing authority certificate (CA certificate) on the RKM appliance.

1. Start a web browser, and connect to the RKM appliance setup page. You will need the URL, and have the proper authority level, a user name, and a password.
2. Select the **Operations** tab.
3. Select **Certificate Upload**.
4. In the **SSLCAcertificateFile** field, enter the full local path of the CA certificate. Do not use the UNC naming convention format.
5. Select **Upload**, **Configure SSL**, and **Restart Webserver**.
6. After the web server restarts, enter the root password.
7. Open another web browser window, and start the RSA management user interface.

   You will need the URL, and have the proper authority level, a user name, and a password.

NOTE
The Identity Group name used in the next step may not exist in a freshly installed RKM. To establish an Identity Group name, click the **Identity Group** tab, and create a name. The name **Hardware Retail Group** is used as an example in the following steps.

8. Select the **Key Classes** tab. For each of the following key classes, perform steps a. through h. to create the class. The key classes must be created only once, regardless of the number of nodes in your encryption group and regardless of the number of encryption groups that will be sharing this RKM.

   kcn.1998-01.com.brocade:DEK_AES_256_XTS

   kcn.1998-01.com.brocade:DEK_AES_256_CCM

   kcn.1998-01.com.brocade:DEK_AES_256_GCM

   kcn.1998-01.com.brocade:DEK_AES_256_ECB

   a. Click **Create**.

   b. Type the key name string into the **Name** field.

   c. Select **Hardware Retail Group** for **Identity Group**.

   d. Deselect **Activated Keys Have Duration**.

   e. Select **AES** for **Algorithm**.

   f. Select **256** for **Key Size**.

   g. Select the **Mode** for the respective key classes as follows:

      XTS for Key Class "kcn.1998-01.com.brocade:DEK_AES_256_XTS"

      CBC for Key Class "kcn.1998-01.com.brocade:DEK_AES_256_CCM"

      CBC for Key Class "kcn.1998-01.com.brocade:DEK_AES_256_GCM"

      ECB for Key Class "kcn.1998-01.com.brocade:DEK_AES_256_ECB"

   h. Click **Next**.

   i. Repeat a. through h. for each key class.

   j. Click **Finish**.

9. For each node, create an identity as follows.

   a. Select the **Identities** tab.

   b. Click **Create**.

   c. Enter a label for the node in the **Name** field. This is a user-defined identifier.

   d. Select the **Hardware Retail Group** in the **Identity Groups** field.

   e. Select the **Operational User** role in the **Authorization** field.

   f. Click **Browse** and select the imported certificate <name>_kac_cert.pem> as the **Identity certificate**.

   g. Click **Save**.

10. Register the RKM key vault on the group leader using the CA certificate for the CA that signed the RKM key vault certificate. The path to the file was entered in the **SSLCAcertificateFile** field. The group leader automatically shares this information with other group members.

```
SecurityAdmin:switch>cryptocfg --import -scp <CA certificate file>
<host IP> <host username> <host path>

SecurityAdmin:switch>cryptocfg --reg -keyvault <CA certificate file>
<RKM IP> primary
```

11. Display the group configuration, using the **cryptocfg - - show -groupcfg** command

RKM Appliance cluster support

When dual RKM appliances are used for high availability, the RKM appliances must be clustered, and must operate in maximum availability mode, as described in the RKM appliance user documentation. Only one RKM key vault should be configured. Do not configure a second RKM key vault from the cluster.

The HP Secure Key Manager

The HP StorageWorks Secure Key Manager (SKM) is a security appliance providing centralized key management operations. SKM runs on a stand-alone FIPS 140-2 level 2 compliant hardware platform that is isolated from the other applications, and runs a hardened operating system. SKM offers high availability, clustering and failover options.

After the required certificate file is loaded on the encryption switch, and the SKM IP addresses are configured on the encryption switch, the encryption switch automatically establishes a secure connection with SKM. Communication with SKM is secured by wrapping DEKs in a master key. The encryption engine must generate its own master key, send DEKs to SKM encrypted in the master key, and decrypt DEKs received from SKM using the same master key.

Setting up an HP SKM key vault consists of registering the encryption group leader and group member nodes with the HP SKM key vault by exporting their KAC certificates, and taking steps on the HP SKM appliance that allow the certificates to be signed by a local certificate authority (CA) on the HP SKM appliance. These steps can be broken down into the following tasks.

Obtaining a signed certificate from the HP SKM appliance software

The following steps describe how to get a signed certificate from the Hewlett Packard Secure Key Manager (HP SKM) appliance. You will need this information when you create a new encryption group with the HP SKM key vault, and you must obtain a signed certificate for each switch.

1. Select **Tools > Internet Options** on your Internet browser.

   Click the **Advanced** tab, and select the **Use TLS 1.0** option.

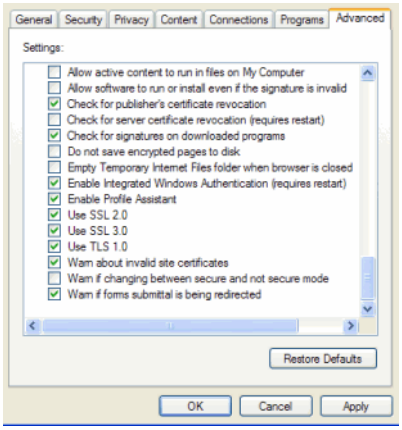

General
Security
Privacy
Content
Connections
Programs
Advanced
Settings:
Allow active content to run in files on My Computer
Allow software to run or install even if the signature is invalid
Check for publisher's certificate revocation
Check for server certificate revocation (requires restart)
Check for signatures on downloaded programs
Do not save encrypted pages to disk
Empty Temporary Internet Files folder when browser is closed
Enable Integrated Windows Authentication (requires restart)
Enable Profile Assistant
Use SSL 2.0
Use SSL 3.0
Use TLS 1.0
Warn about invalid site certificates
Warn if changing between secure and not secure mode
Warn if forms submittal is being redirected
Restore Defaults
OK
Cancel
Apply

FIGURE 155 **TLS 1.0 option from Internet browser**

2. Log in to the HP StorageWorks Secure Key Manager appliance using a browser and https protocol:

   `https://<IP Address>:9443`

   where `10.32.45.13` is the IP address.

   The **HP StorageWorks Secure Key Manager Administrator Authentication** dialog box displays.

3. Enter the user name and password:

   Username: `admin`

   Password: `hpskm028`

   The **Certificate and CA Configuration** dialog box displays.

4. Click the **Security** tab, and then click the **Sign Request** button.

   The **Sign Certificate Request** dialog box displays.

5. Click the **Sign Request** button at the bottom of the screen.

6. Copy and paste the generated certificate contents from the HP SKM into a file. You will import the signed certificate into the switch in the next procedure, "Importing a signed certificate."

Importing a signed certificate

After a signed certificate is obtained, it must be imported and registered.

1. Select a switch from the **Encryption Targets** dialog box, and click the **Properties** tab.

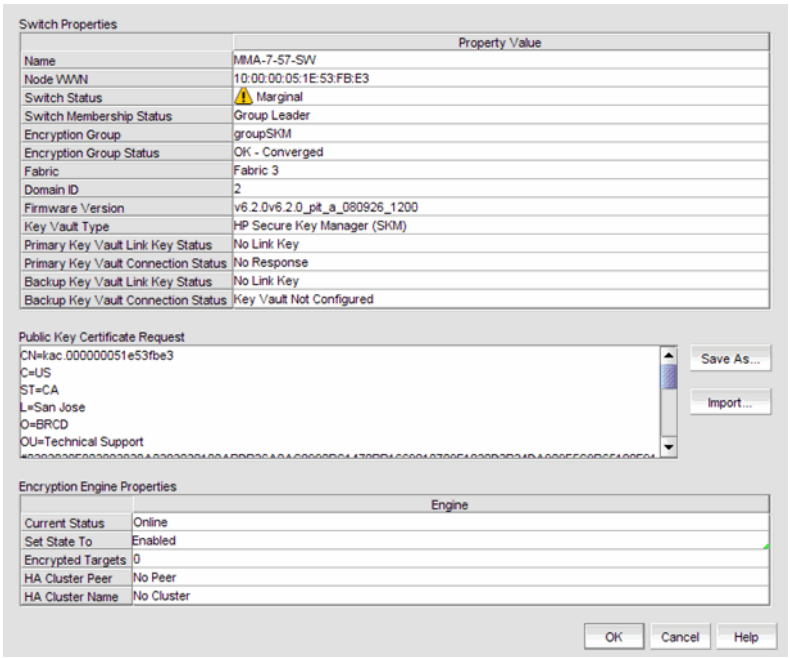


FIGURE 156 **Switch Properties dialog box**

2. Click the **Import** button.

   The **Import Signed Certificate** dialog box displays.

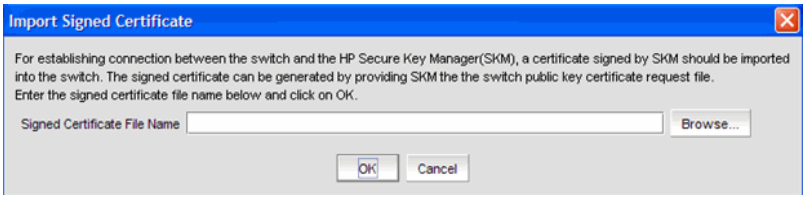

Import Signed Certificate
For establishing connection between the switch and the HP Secure Key Manager(SKM), a certificate signed by SKM should be imported into the switch. The signed certificate can be generated by providing SKM the the switch public key certificate request file.
Enter the signed certificate file name below and click on OK.
Signed Certificate File Name
Browse...
OK
Cancel

FIGURE 157 **Import Signed Certificate dialog box**

3. Browse to the location of the stored, signed certificate, and click **OK**.

   A connection is now established between the switch and the HP Secure Key Manager (SKM).

4. Register the SKM key vault on the group leader using the CA certificate for the CA that signed the SKM key vault certificate. The group leader automatically shares this information with other group members.

```
SecurityAdmin:switch>cryptocfg --import -scp <CA certificate file>
<host IP> <host username> <host path>

SecurityAdmin:switch>cryptocfg --reg -keyvault <CA certificate file>
<RKM IP> primary
```

5. Display the group configuration, using the **cryptocfg --show -groupcfg** command.

Exporting the KAC certificate request

A KAC certificate request must be exported for each encryption node to an SCP-capable host.

1. Log into the group leader as Admin or SecurityAdmin.
2. Set the SKM key vault type by entering the **cryptocfg --set -keyvault** command with the **SKM** option. Successful execution sets the key vault type for the entire encryption group.

```
SecurityAdmin:switch>cryptocfg --set -keyvault SKM
Set key vault status: Operation Succeeded.
```

3. On each node in the encryption group, export the KAC certificate to an SCP-capable host.

```
SecurityAdmin:switch>cryptocfg --export -scp -KACcsr
192.168.38.245 mylogin /tmp/certs/kac_skm.csr
```

NOTE
Record this location so you can easily find the KAC certificate for signing in the "Signing the KAC certificate" procedure.

Setting up a Brocade user

1. Launch the SKM administration console in a web browser and log in with your user name and password.
2. Select the **Security** tab.
3. Select **Local Users & Groups** under **Users and Groups**.

   The **User & Group Configuration** page is displayed.
4. Select **Add** under **Local Users.**
5. Add a new user under **Username**, and a password under **Password**.
6. Select both the **User Administration Permission** and Change **Password Permission** check boxes for the new user.
7. Select **Save** to save this user data.
8. Select **Add** under **Local Groups**.
9. Add a new group called brocade under **Group**.
10. Select **Save**.
11. Select the new brocade group name, and then select **Properties**.

    Local **Group Properties** and a **User List** are displayed.
12. In the **User List** section, select or type the Brocade user name under **Username**.
13. Select **Save**.

    The Brocade user is now configured on SKM.

Registering the Brocade user name and password on the switch

You must register the user name and password that was added to the SKM appliance in "Setting up a Brocade user" on the switch.

1. Register a user password and user name by issuing the following command at the switch.

   ```
   SecurityAdmin:switch>cryptocfg  --reg -KAClogin
   ```

2. When prompted, enter the user name specified in step 5 of "Setting up a Brocade user".
3. When prompted enter and confirm the password specified in step 5 of "Setting up a Brocade user".

Setting up the local certificate authority

The local certificate authority is set up by adding Brocade to the Local Certificate Authority List. After establishing the local certificate authority for Brocade, Brocade is then added and accepted as a trusted user of SKM.

1. Select the **Security** tab on the SKM key manager.
2. Select **Local CAs** under **Certificates and CAs**.

   The **Certificate and CA Configuration** page is displayed. This page includes the **Local Certificate Authority List**, and a **Create Local Certificate Authority** dialog box.

3. Enter the following in the **Create Local Certificate Authority** dialog box:
   - Certificate Authority Name - HPSKM_CA1
   - Common Name - HPSKM_CA1
   - Organization Name - Brocade
   - Organizational Unit Name - Storage Software
   - Locality Name - SJC
   - State or Province Name - CA
   - Country Name - US
   - Email Address - support@brocade.com
   - Key Size - 2048
   - Certificate Authority Type - Select Self-Assigned Root CA. The values for CA certification Duration and Maximum User Certificate Duration should both be 3650.

NOTE
The names shown are only examples. You may use different names. Remember the **Certificate Authority Name**, or write it down. You will need later in the procedures for "Adding the local CA to the trusted CAs list", "Adding a server certificate for the SKM appliance", and "Downloading the local CA certificate file".

4. Click **Create**.

   Successful completion is indicated when the new Local CA appears on the **Local Certificate Authority** List.

Adding the local CA to the trusted CAs list

You must now update the Trusted CAs list with the local CA name you created in "Setting up the local certificate authority".

1. Select the **Security** tab on the SKM key manager.
2. Select **Trusted CA Lists** under **Certificates and CAs**.

   The **Trusted CA Lists** page is displayed.
3. Select **Default** under **Profile Name**.
4. Click **Properties**.

   A properties dialog box is displayed.
5. Click **Edit**.

   A dialog box is displayed that allows you to **Add** CAs to a **Trusted CAs** list from a list of **Available CAs**, or to **Remove** CAs from the **Trusted CAs** list and place them in the list of **Available CAs**.
6. In the **Available CAs** list, select the local CA name you created and click **Add** to move the CA name to the **Trusted CAs** list.
7. Click **Save**.

Adding a server certificate for the SKM appliance

A server certificate must be created for the SKM appliance.

1. Select the **Security** tab on the SKM key manager.
2. Select **Certificates** under **Certificates and CAs**.

   The **Certificate and CA Configuration** page is displayed. This page includes a **Create Request Information** dialog box.
3. Enter the following in the **Create Request Information** dialog box:
   - Certificate Name - HPSKM_Server_029
   - Common Name - HPSKM_Server_029
   - Organization Name - Brocade
   - Organizational Unit Name - Storage Software
   - Locality Name - SJC
   - State or Province Name - CA
   - Country Name - US
   - Email Address - support@brocade.com
   - Key Size - 2048

NOTE
The names shown are examples. You may use other names. Remember the **Certificate Name**, or write it down. You will need it later in the procedure for "Downloading the local CA certificate file".

4. Select **Create Certificate Request**.

   Successful completion is indicated when the new entry for the server certificate appears on the **Certificate List** with a **Certificate Status** of **Request Pending**.

5. Select the pending server certificate from the list.
6. Select **Properties**.

   A **Certificate Request Information** dialog box is displayed.

7. Copy the key contents, beginning with `---BEGIN CERTIFICATE REQUEST---` and ending with `---END CERTIFICATE REQUEST---`. Be careful not to include any extra characters.
8. Select **Local CAs** under **Certificates and CAs**.

   The **Certificate and CA Configuration** page is displayed.

9. Select the local certificate name from the **CA Name** column.
10. Select **Sign Request**.

    A **Sign Certificate Request** dialog box is displayed.

11. Select **Sign with Certificate Authority** using the CA name with a maximum of 3649 days.
12. Select **Certificate Purpose - Server** and enter 3649 as the **Certificate Duration**.
13. Paste the key contents you previously copied in step 7 into the **Certificate Response** window.
14. Select **Sign Request**.
15. Copy the key contents, beginning with `---BEGIN CERTIFICATE REQUEST---` and ending with `---END CERTIFICATE REQUEST---`. Be careful not to include any extra characters.
16. From the **Security** tab, **Certificates and CAs**, select **Certificates**. From the certificate list, select the name of the certificate being signed.
17. Select **Install Certificate**.
18. Paste the certificate data from step 15, and select **Save**. The certificate status is now Active.

Downloading the local CA certificate file

This procedure requires selection of the local certificate authority name (CA name) created using the "Setting up the local certificate authority" procedure. Have the CA name available so you will be able to select the correct name from the **Local Certificate Authority List**. This procedure also requires you to enter the server certificate name created using the "Adding a server certificate for the SKM appliance" procedure. Be sure to have the server certificate name available.

1. Select the **Security** tab on the SKM key manager.
2. Select **Local CAs** under **Certificates and CAs**.

   The Certificate and CA Configuration page is displayed.

3. Select the local certificate name from the **CA Name** column in the **Local Certificate Authority List.**
4. Select **Download**.
5. After the download completes, save the file locally, and rename the file to change the file extension from .cert to .pem (e.g., from hpskm_cal.cert to hpskm_cal.pem).

6. Select the **Device** tab on the SKM key manager.
7. Select **KMS Server** under **Device Configuration**.

   The **Key Management Services Configuration** page is displayed.
8. Select **Edit** under **KMS Server Settings**.
9. Click the check boxes for the following:
   - **Use SSL**
   - **Allow Key and Policy Configuration Operations**
   - **Allow Key Export**
10. Type in the server certificate name in the **Server Certificate** field.
11. Select **Save** to save these settings.
12. Select **Edit** under **KMS Server Authentication Settings**.
13. Select **Required** for **Password Authentication**.
14. Select **Save** to save these settings.

Creating an SKM Key vault High Availability cluster

The HP SKM key vault supports clustering of HP SKM appliances for high availability. If two SKM key vaults are configured, they must be clustered. If only a single LKM key vault is configured, it may be clustered for backup purposes, but it will not be directly used by the switch.

To create a cluster, perform the following steps on one of the HP SKM appliances that is to be a member of the cluster

1. Select the **Device** tab on the SKM key manager.
2. Select **Cluster** under **Device Configuration**.

   The **Cluster Configuration** page is displayed.
3. Type the cluster password under **Create Cluster**.

   The default value for **Local Port** is 9001. This is the recommended value, and should not be changed unless your IT department requires a different value.
4. Select **Create**.
5. Select **Download Cluster Key** under **Cluster Settings**.
6. Copy the cluster key and save it in a convenient location. This key is needed for "Adding an HP SKM appliance to a cluster". You will be able to browse to the location as part of that procedure.

NOTE
Record the local IP address and cluster password for use in "Adding an HP SKM appliance to a cluster".

Copying the local CA certificate

1. Select the **Security** tab.
2. Select **Local CAs** under **Certificates & CAs**.
3. Select the name of the local CA from the **Local Certificate Authority** list.

   The **CA Certificate Information** is displayed.
4. Copy the key contents, beginning with `---BEGIN CERTIFICATE REQUEST---` and ending with `---END CERTIFICATE REQUEST---`. Be careful not to include any extra characters.

   This certificate data will be transferred to other HP SKM appliances in "Adding an HP SKM appliance to a cluster".

   Keep this browser window open while going on to "Adding an HP SKM appliance to a cluster".

Adding an HP SKM appliance to a cluster

1. Open a new browser window, while keeping the browser window from"Copying the local CA certificate" open.
2. Log in to the HP SKM Key Manager console of the HP SKM appliance that is being added.
3. Select the **Security** tab.
4. Select **Known CAs** under **Certificates & CAs**.

   The **Certificate and CA Configuration** page is displayed.
5. Type the certificate name in the **Certificate Name** field under **Install CA certificate**.
6. Paste the certificate data you copied previously in the "Copying the local CA certificate" procedure. If you kept the browser window open as suggested in "Copying the local CA certificate", the same data is available in that browser window.
7. Select **Install**.
8. From the HP SKM key manager main page, select the **Device** tab.
9. Select **Cluster** under **Device Configuration**.
10. Select **Join Cluster**.
11. Type the original cluster member's IP address into **Cluster Member IP**. This is the IP address designated as the local IP address that you recorded for this step in "Creating an SKM Key vault High Availability cluster"
12. Browse to the location of the temporary cluster key file that you copied in "Creating an SKM Key vault High Availability cluster" for the **Cluster Key File**.
13. Type the cluster password you recorded in "Creating an SKM Key vault High Availability cluster" as the **Cluster Password**.

14. Select **Join**.
15. You are prompted to confirm the operation. Select **Confirm**.

    The **Cluster Configuration** page displays, showing the cluster members.

    Repeat the procedure to add more members, as needed. Delete the temporary cluster key file when finished. You should also verify that the same server certificate configured for all cluster members by selecting the **Device** tab, and select **KMS Server Settings**.

Signing the KAC certificate

The KAC certificate exported by the encryption switch or blade must be signed using the certificate authority created in the "Setting up the local certificate authority" procedure.

1. Go to the location where the kac_skm_req.csr file was downloaded on an SCP-capable host. You should have this location recorded and available, as described in "Exporting the KAC certificate request".
2. Open the file and copy the contents, beginning with `---BEGIN CERTIFICATE REQUEST---` and ending with `---END CERTIFICATE REQUEST---`. Be careful not to include any extra characters.
3. On the SKM key manager main page, select the **Security** tab.
4. Select **Local CAs** under **Certificates & CAs**.

   The **Certificate and CA Configuration** page is displayed.
5. Under **Local Certificate Authority List**, select the CA Name for the CA created in "Setting up the local certificate authority".
6. Select **Sign Request**.

   The **Sign Certificate Request** page is displayed.
7. Select **Sign with Certificate Authority** using the CA name with the maximum of 3649 days option.
8. Select **Client** as **Certificate Purpose**.
9. Allow Certificate **Duration** to default to 3649.
10. Paste the file contents that you copied in step 2 in the **Certificate Request Copy** area.
11. Select **Sign Request**.

    Upon success, you are presented with the option of downloading the signed certificate.
12. Download the signed certificate to your local system as signed_kac_skm_cert.pem.

    This file is then ready to be downloaded to the encryption switch or blade.

Importing a signed certificate (SAN Management program)

The public key certificate from the switch is used to authenticate connections to the key vault.

1. Select a switch from the **Encryption Targets** dialog box, and click the **Properties** tab.

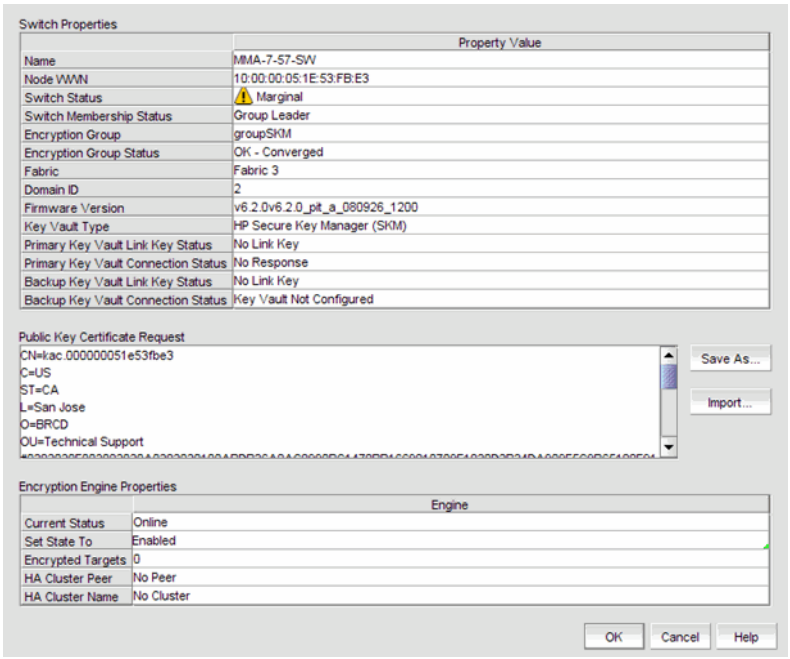


FIGURE 158 Switch Properties dialog box

2. Click the **Import** button.

   The **Import Signed Certificate** dialog box displays.

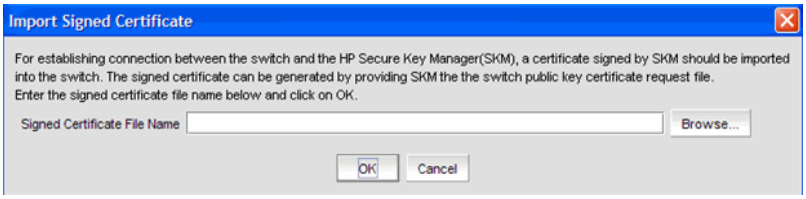

Import Signed Certificate
For establishing connection between the switch and the HP Secure Key Manager(SKM), a certificate signed by SKM should be imported into the switch. The signed certificate can be generated by providing SKM the the switch public key certificate request file.
Enter the signed certificate file name below and click on OK.
Signed Certificate File Name
Browse...
OK
Cancel

FIGURE 159 Import Signed Certificate dialog box

3. Browse to the location of the stored, signed certificate, and click **OK**.

   A connection is now established between the switch and the HP Secure Key Manager (SKM).

Thales Encryption Manager for Storage

Communication with the Thales Encryption Manager for Storage (TEMS) is referred to as NCKA in operational descriptions in this appendix. NCKA is secured by wrapping DEKs in a master key. The encryption engine must generate its own master key, send DEKs to NCKA encrypted in the master key, and decrypt DEKs received from NCKA using the same master key. The master key may optionally be stored as a key record in the NCKA key vault as a backup, but NCKA does not assume responsibility for the master key. The master key must be backed up and stored, and policies and procedures for responding to theft or loss must be in place.

Adding a client

Communication must be over an SSL connection. This requires creation of a client certificate signed by a Certificate Authority (CA) on the key vault. It is assumed that a CA has been created by an officer at the keyvault, and a CA certificate has been generated. Also, a group must be created for Brocade by an administrator. This group must exist and is the only supported group for the Brocade encryption switch and blade. Details about how to set up a CA and a group can be found in Thales documentation.

NOTE
Each Thales key vault has both a management IP address and a data IP address. Clients must communicate with the key vaults using the data IP address.

1. Generate a user password and user name by issuing the following CLI command at the switch:

   ```
   cryptocfg  --reg -KAClogin
   ```

   This command will print out the user name, and then prompt you to create a password. Save the user name and password.
2. Invoke the Thales key vault web browser and log in as manager.
3. Click the **Client** tab.
4. Click the **Add Client** tab.
5. Enter the user name from step one in the **Name** field.
6. Enter the password from step one in the **Password** and **Verify Password** fields.
7. Select the group **brocade** from the **group** menu.
8. Click **Add Client**.

   A client user is created. Verify the user just created is listed in the table.

Signing the CSR

1. Export the certificate signing request (CSR) certificate from the switch.

   ```
   Cryptocfg -export -scp -KACsr <host IP> <user name> <file path>
   ```

NOTE
On some host systems this request does not work. If that is true for your system, copy the .csr file above manually to the workstation you are using to interface with the key vault.

2. Under the **certificate** column in the user table, click on the pen icon for the newly created user.

   The **Sign Certificate Request** page is displayed.

3. Either enter the .csr file name exported from the switch in the above steps in the **From file** box, or cut and paste the .csr file contents to the **From text** box and click **sign**.

4. Under the **Certificate** column click on the export icon (globe with an arrow).

   A web browser file save dialog displays

5. Click **save** and enter the destination location for this signed certificate. For example; brcduser1@ncka-1.pem for the primary keyvault and brcduser1@ncka-2.pem for the secondary keyvault.

6. Perform the above steps for both the primary and secondary key vaults using the same user name, password, and group.

NOTE
the same CSR file is used for both the primary and secondary key vaults; however, the signed certificate exported from the two key vaults are different and must be independently registered as indicated in the steps below.

7. Import the signed certificates back into the switch.

   ```
   cryptocfg -import -scp <local file> <host IP> <host user name> <host file
   path>
   ```

NOTE
On some systems the scp (secure copy) may not work, in this case copy the signed certificate file above to: /etc/fabos/certs/mace/

8. Repeat steps one through six for all member nodes in the encryption group.

Registering the certificates

Examples below are for the two Thales key vaults installed. Commands assume the exported signed certificates were saved as brcduser1@ncka-1 and brcduser1@ncka-2 for the primary and secondary key vaults and the data port IP addresses are 10.32.44.112 and 10.32.44.114.

1. Set the key vault type.

```
cryptocfg --set -keyvault NCKA
```

2. Register the signed KAC certificates.

```
cryptocfg --reg -KACcert brcduser1@ncka-1.pem primary
cryptocfg -reg -KACcert brcduser1@ncka-2.pem secondary
```

3. Register the primary and secondary key vault certificates and data port IP addresses.

```
cryptocfg --reg -keyvault NCKA_CA1 brcduser1@ncka-1.pem 10.32.44.112 primary
cryptocfg --reg -keyvault NCKA_CA2 brcduser1@ncka-2.pem 10.32.44.114 secondary
```

NOTE
The signed certificate file contains both the client and keyvault CA certificates so the same file name is used for both the keyvault and KACcert registration.

4. Repeat steps one and two for each encryption group member.
5. Display the group configuration to verify values

```
cryptocfg --show -groupcfg
```

Appendix

Sybase and Derby Database Fields

B

In this appendix

- Capability 456
- Client_view 457
- Collector 460
- Config 463
- Connected end devices 465
- Device 466
- EE- Monitor 473
- Event/FM 475
- Fabric 481
- FC Port Stats 484
- FCIP 487
- FCIP Tunnel Stats 490
- GigE Port Stats 492
- ISL 494
- License 497
- Meta SAN 498
- Network 500
- Others 501
- Port Fencing 502
- Quartz 503
- Reports 506
- Role Based Access Control 506
- SNMP 509
- Stats 512
- Switch 514
- Switch details 519
- Switch port 524
- Threshold 531
- User Interface 532
- Zoning 1 533
- Zoning 2 535

Database tables and fields

Capability

TABLE 46 CAPABILITY_

Field	Definition	Format	Size
NAME *	Name of the capability.	varchar	256
DESCRIPTION	Optional detailed description about the capability.	varchar	512

TABLE 47 CARD_CAPABILITY

Field	Definition	Format	Size
CARD_ID *	DB ID of the card.	int	
CAPABILITY_ *	Name of the capability detected on the card.	varchar	256
ENABLED	1 = the capability is enabled on the card.	int	

TABLE 48 VIRTUAL_SWITCH_CAPABILITY

Field	Definition	Format	Size
VIRTUAL-SWITCH_ID *	DB ID of virtual switch.	int	
CAPABILITY_ *	Name of capability detected on virtual switch.	varchar	256
ENABLED	1 = the capability is enabled on the virtual switch.	int	

TABLE 49 CARD

Field	Definition	Format	Size
ID *		int	
CORE_SWITCH_ID *	Core switch DB ID.	int	
SLOT_NUMBER	The number of the physical slot in the chassis where the blade is plugged in. For fixed blades, SlotNumber is zero.	smallint	
TYPE	ID of the blade to identify the type.	smallint	
EQUIPEMNT_TYPE	The type of the blade. It is either SW BLADE or CP BLADE.	varchar	16
STATE	State of the blade, such as ENABLED or DISABLED.	varchar	32
POWER_STATE	State of power supply to the blade.	varchar	16
ATTN_STATE		varchar	32
SERIAL_NUMBER	Factory serial number of the blade.	varchar	32
PART_NUMBER	The part number assigned by the organization responsible for producing or manufacturing the blade.	varchar	32
TRUNKING_SUPPORTED	1 = trunking is supported on this blade.	smallint	
FICON_DISABLED	1 = FICON is disabled on this blade.	smallint	
IP_ADDRESS	IP address of first Ethernet management port for a given slot with intelligent blade.	char	64
SUBNET_MASK	Mask of first Ethernet man.agement port for a given slot with intelligent blade.	varchar	64
DEFAULT_GATEWAY	Gateway IP address Ethernet management for a given slot with intelligent blade.	varchar	64
PRIMARY_FW_VERSION	Primary firmware version of applications on this blade. Applicable only for AP_BLADE.	varchar	48
SECONDARY_FW_VERSION	Secondary firmware version applications on this blade. Applicable only for AP_BLADE.	varchar	48

TABLE 50 CORE_SWITCH_CAPABILITY

Field	Definition	Format	Size
CORE_SWITCH_ID *	DB ID.	int	
CAPABILITY_ *	Name of the capability detected on the core switch.	varchar	256
ENABLED	1 = the capability is enabled on the core switch.	int	

Client_view

TABLE 51 USER_

Field	Definition	Format	Size
NAME *	User name.	varchar	128
DESCRIPTION	User description.	varchar	512

TABLE 51 USER_ (Continued)

Field	Definition	Format	Size
PASSWORD	User password.	varchar	128
EMAIL	User e-mail ID.	varchar	1024
NOTIFICATION_ENABLED	Flag for e-mail notification.	smallint	

TABLE 52 USER_PREFERENCE

Field	Definition	Format	Size
USER_NAME *	User name whose preferences are saved. It corresponds to user_name in USER_table.	varchar	128
CATEGORY *	The name for a set of related preferences.	varchar	128
CONTENT	The set of preferences saved as name-value pairs.	long varchar	

TABLE 53 CLIENT_VIEW

Field	Definition	Format	Size
ID *		int	
USER_NAME	The Management application user name.	varchar	128
NAME	Client view name.	varchar	255
DESCRIPTION	Client View description.	varchar	255

TABLE 54 CLIENT_VIEW_COLUMN

Field	Definition	Format	Size
ID *		int	
NAME	Column name.	varchar	255
ENTITY_CATEGORY	Either "fabric" or "product (switch or device)" or "port"; or combination of these 3 basic categories.	varchar	128
COLUMN_INDEX	0 = Predefined column. 1 = First user-defined column. 2 = Second user-defined column. 3 = Third user-defined column.	small int	
DESCRIPTION	Column description, typically populated for user-defined columns.	varchar	255
ICON_ID	Not used.	int	
VISIBLE	1 = all predefined / fixed columns. 0 = user-defined columns.	smallint	
EDITABLE	1 = column is editable. 0 = column is not editable.	smallint	

TABLE 55 CLIENT_VIEW_MEMBER

Field	Definition	Format	Size
CLIENT_VIEW_ID *	Foreign key to CLIENT_VIEW table.	int	
FABRIC_ID *	Foreign key to FABRIC table.	int	

TABLE 56 FABRIC

Field	Definition	Format	Size
ID *		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256
TYPE	Type of fabric: 0 = legacy fabric. 1 = base fabric. 2 = logical fabric.	smallint	
SECURE	1 = it is a secured fabric.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone configuration which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

Collector

TABLE 57 FABRIC_CHECKSUM

Field	Definition	Format	Size
FABRIC_ID *	Fabric ID, foreign key to the FABRIC table.	int	
CHECKSUM_KEY *	Type of checksum, e.g. device data or zone data.	varchar	32
CHECKSUM	Actual checksum value.	varchar	16

TABLE 58 FABRIC_COLLECTION

Field	Definition	Format	Size
FABRIC_ID *	Fabric ID, foreign key to the FABRIC table.	int	
COLLECTOR_NAME *	Name of the collector, e.g., NameServerInfoCollector, TopologyCollector, ZoneInfoCollector, ActiveZoneInfoCollector.	varchar	256
SEED_SWITCH_IP	IP address of the switch which serves as the seed switch. This is the switch from which above mentioned fabric level collectors get their information.	varchar	128
LAST_SEED_SW_ MODIFICATION	Timestamp of the seed switch, when the particular HTML page was changed last. Note that this is not when the last time collection was done.	timestamp	

TABLE 59 COLLECTOR

Field	Definition	Format	Size
NAME *	Name of the collector registered with the collection framework.	varchar	256
CLASS_NAME	Java class name which serves as the collector.	varchar	256
DESCRIPTION	Collector description, usually not used.	varchar	512

TABLE 60 FABRIC

Field	Definition	Format	Size
ID *		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256
TYPE	Type of fabric (0:legacy fabric, 1: base fabric, 2: logical fabric).	smallint	
SECURE	1 = it is a secured fabric.	smallint	

TABLE 60 FABRIC (Continued)

Field	Definition	Format	Size
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted,i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone configuration which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

TABLE 61 COLLECTOR_END_TIMESTAMP

Field	Definition	Format	Size
COLLECTOR_SOURCE *	Internal key for switches and fabrics for which collection is undertaken.	varchar	256
COLLECTOR_NAME *	Collection name, Java class used to collect specific fabric or switch information.	varchar	256
TIMESTAMP_	When the last successful collection is done.	timestamp	
LAST_COLLECTED_STATUS	Status of the last collection, successful or not. 200 is for successful. Values are standard HTTP protocol values.	smallint	

TABLE 62 VIRTUAL_SWITCH_COLLECTION

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID *	DB ID of virtual switch.	int	
COLLECTOR_NAME *	Collector name.	varchar	256
LAST_VIRTUAL_SW_ MODIFICATION	Last modified time on switch.	timestamp	

TABLE 63 VIRTUAL_SWITCH_CHECKSUM

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID *	DB ID of virtual switch.	int	
CHECKSUM_KEY *	Checksum key.	varchar	32
CHECKSUM	Checksum value.	varchar	16

TABLE 64 CORE_SWITCH_CHECKSUM

Field	Definition	Format	Size
CORE_SWITCH_ID *	DB ID.	int	
CHECKSUM_KEY *	Checksum type.	varchar	32
CHECKSUM	Checksum value.	varchar	16

TABLE 65 CORE_SWITCH_COLLECTION

Field	Definition	Format	Size
CORE_SWITCH_ID *	Core switch ID.	int	
COLLECTION_NAME *	Collector name.	varchar	256
LAST_CORE_SW_ MODIFICATION	Last core switch modification time.	timestamp	

TABLE 66 SECURITY_POLICY

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID *	DB ID of virtual_switch.	int	
POLICY_NUMBER*	IPSec Policy Number. The number can range from 1 to 32.	smallint	
POLICY_TYPE*	Type of the Policy. The possible values are IKE or IPSec	smallint	
ENCRYPTION_ALGORITHM	Encryption Algorithm for the policy.The following are the possible Encryption: NONE,DES,3DES,AES-128,AES-256,AES-CM-128 or AES-CM-256.	varchar	32
AUTHENTICATION_ALGORITHM	Authentication Algorithm for the policy: NONE SHA-1 MD5 AES-XCBC	varchar	32
PERFECT_FORWARD_POLICY_ENABLED	Perfect Forward Secrecy for the policy. The possible values are 0 or 1.	smallint	
DIFFIE_HELLMAN_GROUP	Diffie-Hellman Group used in PFS negotiation.	smallint	
SECURITY_ASSOC_LIFE	Association lifetime in seconds.	double	
SECURITY_ASSOC_LIFE_IN_MB	Security association lifetime in megabytes.	double	

Config

TABLE 67 FIRMWARE_SWITCH_DETAIL

Field	Definition	Format	Size
FIRMWARE_ID*	ID for the firmware file.	int	
SWITCH_TYPE*	Switch type that supports this firmware file.	smallint	
REBOOT_REQUIRED	Reboot required flag for the switch type.	smallint	
NUMFILES	Number of files in the firmware.	int	

TABLE 68 FIRMWARE_FILE_DETAIL

Field	Definition	Format	Size
ID*		int	
FIRMWARE_NAME	Name of the firmware file.	varchar	64
MAJOR_VERSION	Major version bit from the firmware version.	smallint	
MINOR_VERSION	Minor version bit from the firmware version.	smallint	
MAINTENANCE	Maintenance bit from the firmware version.	smallint	
PATCH	Patch bit from the firmware version.	varchar	64
PHASE	Phase bit from the firmware version.	varchar	64

TABLE 68 FIRMWARE_FILE_DETAIL (Continued)

Field	Definition	Format	Size
RELEASE_DATE	Release date of the firmware file.	timestamp	
IMPORTED_DATE	Imported date of the file to the Management application.	timestamp	
FIRMWARE_FILE_SIZE	Firmware file size.	int	
FIRMWARE_LOCATION	Firmware file location in the Management application repository.	varchar	1024
RELEASE_NOTES_ LOCATION	Release notes file location in the Management application repository.	varchar	1024
FIRMWARE_REPOSITORY_ TYPE	Repository type to identify the FTP server: 0 = internal FTP. 1 = external FTP.	smallint	

TABLE 69 SWITCH_PLATFORM

Field	Definition	Format	Size
SWITCH_TYPE*	Switch type.	smallint	
DESCRIPTION	Description of the switch type.	varchar	256
SPEED	Switch maximum speed.	smallint	
MULTI_CP_CAPABLE	Switch is multi-CP capable or not.	smallint	

TABLE 70 FTP_SERVER

Field	Definition	Format	Size
ID*		int	
TYPE	Type indicates the FTP is internal or external. 0 = internal. 1 = external.	smallint	
IP	FTP server IP address.	varchar	64
USER_NAME	FTP server user name.	varchar	64
PASSWORD	FTP server user password.	varchar	64
ROOT_DIRECTORY	FTP server root directory location.	varchar	1024
PORT	Port on which FTP server is configured.	int	

TABLE 71 SWITCH_TYPE_FIRMWARE_VERSION

Field	Definition	Format	Size
SWITCH_TYPE*	Switch type.	smallint	
MIN_FOS_VERSION*	Supported minimum firmware version.	varchar	64
MAX_FOS_VERSION	Supported maximum firmware version.	varchar	64

TABLE 72 SWITCH_CONFIG

Field	Definition	Format	Size
NAME	Name of the switch configurations uploaded from the switch either on demand or through scheduler.	int	
ID*		varchar	64
SWITCH_ID	ID of the switch from which the configuration has been uploaded.	int	
BACKUP_DATE_TIME	The date/time stamp at which the configuration has been uploaded.	timestamp	
CONFIG_DATA	The actual switch configuration data.	longvarchar	
KEEP_COPY	The column value (1) helps to preserve the configuration even after the expiration of its age.	smallint	
CREATED_BY	The column value helps to figure out who triggered the configuration upload operation.	varchar	64

Connected end devices

TABLE 73 CED_APPLICATION

Field	Definition	Format	Size
ID*		int	
NAME	Name of the application. Application represents a collection of active zones in a fabric.	varchar	24
FABRIC_ID	ID of the fabric for which the application is created.	int	

TABLE 74 CED_APPLICATION_MEMBER

Field	Definition	Format	Size
APPLICATION_ID*	Auto-generated DB CED_Application table ID.	int	
ZONE_ID*	Auto-generated DB Zone table ID which joins as a member of the application.	int	

TABLE 75 CED_USER_PREFERENCE

Field	Definition	Format	Size
USER_NAME*	User Name carried from _USER table.	varchar	128
FABRIC_ID*	Fabric ID carried from Fabric table.	int	
APPLICATION_ID	CED application ID representing the group of end devices to be displayed in the fabric.	int	

Device

TABLE 76 DEVICE_PORT

Field	Definition	Format	Size
ID*		int	
NODE_ID	DB ID of the device node to which this port belongs.	int	
DOMAIN_ID	Domain ID of the switch to which this device port is attached.	int	
WWN	Device port WWN.	char	23
SWITCH_PORT_WWN	WWN of the switch port to which this device port is attached.	char	23
NUMBER	Switch port number to which this device is attached.	smallint	
PORT_ID	Device port ID.	varchar	6
TYPE	Device port type, such as N or NL.	varchar	32
SYMBOLIC_NAME	Device port symbolic name.	varchar	256
FC4_TYPE	FC payload protocol.	varchar	16
COS	FC class of service.	varchar	16
IP_PORT		varchar	63
HARDWARE_ADDRESS		varchar	6
TRUSTED	1 if found at discovery time or user has entrusted this device port explicitly.	smallint	
CREATION_TIME	When the device port was discovered, i.e., created in the DB.	timestamp	
MISSING	1 if that device port is missing from the fabric.	smallint	
MISSING_TIME	Time when it misses.	timestamp	
NPV_PHYSICAL	Update NPV device type on this given device port. The value "npvPhysical" on the device port will be 1 when the device port has reference to a device node of DEVICE_TYPE value 0 i.e. physical. It points to a switch port to which at least one other device port points; and that other pointing device port has reference to a device node of DEVICE_TYPE value 2 (NPV).	smallint	

TABLE 77 FICON_DEVICE_PORT

Field	Definition	Format	Size
DEVICE_PORT_ID*	Value for the device port to which these FICON properties are applied.	int	
TYPE_NUMBER		varchar	16
MODEL_NUMBER	Ficon device model number, such as S18.	varchar	64
MANUFACTURER	Manufacturer of the device, typically IBM.	varchar	64
MANUFACTURER_PLANT	Plant number where the device is manufactured.	varchar	64
SEQUENCE_NUMBER	Device sequence number.	varchar	32

TABLE 77 FICON_DEVICE_PORT (Continued)

Field	Definition	Format	Size
TAG	FICON device property, e.g., 809a or 809b.	varchar	16
FLAG	FICON device property, e.g., 0x10 (hex).	varchar	8
PARAMS	FICON device property string, e.g., Valid channel port.	varchar	16

TABLE 78 DEVICE_NODE

Field	Definition	Format	Size
ID*		int	
FABRIC_ID	Fabric DB ID to which this device node belongs.	int	
WWN	Device node WWN.	char	23
TYPE	Initiator or target or both or unknown.	varchar	32
DEVICE_TYPE	0 = physical 1 = virtual 2 = NPV 3 = iSCSI 4 = both physical & virtual	smallint	
SYMBOLIC_NAME	Device node symbolic name.	varchar	256
FCMI_HOST_NAME	Device node FDMI host name.	varchar	128
VENDOR	Device node vendor.	varchar	64
CAPABILITY_		varchar	16
TRUSTED	1 = the node is trusted for "fabric tracking."	smallint	
CREATION_TIME	Timestamp when the record is created by the Management application server.	timestamp	
MISSING	1 = the device node is missing from the fabric.	smallint	
MISSING_TIME	Time when the device node missed.	timestamp	
PROXY_DEVICE	One of the device ports of this device node has translated domain. That device port is set as the Proxy Device and this Device Node is treated as virtual by assigning a value of 1 to this field.	smallint	
AG	1 = the device node is actually an AG connected to a switch in the fabric.	smallint	

TABLE 79 DEVICE_ENCLOSURE_MEMBER

Field	Definition	Format	Size
ENCLOSURE_ID*	DEVICE_ENCLOSURE table ID.	int	
DEVICE_PORT_WWN*	Comment on column DEVICE_ENCLOSURE_MEMBER.DEVICE_PORT_WWN is 'WWN Of Device Port'.	char	23
DEVICE_PORT_ID	Device_Port table ID.	int	

TABLE 80 DEVICE_ENCLOSURE

Field	Definition	Format	Size
ID*		int	
FABRIC_ID	ID of the fabric to which the device enclosure belongs.	int	
NAME	Name of the Device enclosure.	varchar	256
TYPE	Type of Device enclosure - Storage Array/Server.	varchar	32
ICON	Type of Icon.	int	
OS	Operating System.	varchar	256
APPLICATIONS	Application which created device enclosure.	varchar	256
DEPARTMENT	Department using this device enclosure.	varchar	256
CONTACT	Contact person details.	varchar	256
LOCATION	Location of physical setup.	varchar	256
DESCRIPTION	Description if any.	varchar	256
COMMENT	Comments if any.	varchar	256
IP_ADDRESS	IP Address if assigned by user.	varchar	128
VENDOR	Vendor name.	varchar	256
MODEL	Device enclosure Model.	varchar	256
SERIAL_NUMBER	Serial Number given for the entity.	varchar	256
FIRMWARE	Firmware running on the device which is not applicable for device enclosure logical entity.	varchar	256
USER_DEFINED_VALUE1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE3	User-defined custom value.	varchar	256

TABLE 81 FABRIC

Field	Definition	Format	Size
ID*		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256
TYPE	Type of fabric: 0 = legacy fabric 1 = base fabric 2 = logical fabric	smallint	

TABLE 81 FABRIC (Continued)

Field	Definition	Format	Size
SECURE	1 = it is secured fabric.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when the fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when the fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone configuration which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

TABLE 82 DEVICE_PORT_INFO

Name	Source
ID	DEVICE_PORT.ID
NODE ID	DEVICE_PORT.NODE_ID
DOMAIN ID	DEVICE_PORT.DOMAIN_ID
WWN	DEVICE_PORT.WWN
SWITCH PORT WWN	DEVICE_PORT.SWITCH_PORT_WWN
NUMBER	DEVICE_PORT.NUMBER
PORT ID	DEVICE_PORT.PORT_ID
TYPE	DEVICE_PORT.TYPE
SYMBOLIC NAME	DEVICE_PORT.SYMBOLIC_NAME
FC4 TYPE	DEVICE_PORT.FC4_TYPE
COS	DEVICE_PORT.COS
IP PORT	DEVICE_PORT.IP_PORT
HARDWARE ADDRESS	DEVICE_PORT.HARDWARE_ADDRESS
TRUSTED	DEVICE_PORT.TRUSTED
CREATION TIME	DEVICE_PORT.CREATION_TIME
MISSING	DEVICE_PORT.MISSING

TABLE 82 DEVICE_PORT_INFO

Name	Source
MISSING TIME	DEVICE_PORT.MISSING_TIME,
NPV PHYSICAL	DEVICE_PORT.NPV_PHYSICAL
TYPE NUMBER	FICON_DEVICE_PORT.TYPE_NUMBER
MODEL NUMBER	FICON_DEVICE_PORT.MODEL_NUMBER
MANUFACTURER	FICON_DEVICE_PORT.MANUFACTURER
MANUFACTURER PLANT	FICON_DEVICE_PORT.MANUFACTURER_PLANT
SEQUENCE NUMBER	FICON_DEVICE_PORT.SEQUENCE_NUMBER
TAG	FICON_DEVICE_PORT.TAG
FLAG	FICON_DEVICE_PORT.FLAG
PARAMS	FICON_DEVICE_PORT.PARAMS
NAME	USER_DEFINED_DEVICE_DETAIL.NAME
USER DEFINED TYPE	USER_DEFINED_DEVICE_DETAIL.TYPE
IP ADDRESS	USER_DEFINED_DEVICE_DETAIL.IP_ADDRESS
CONTACT	USER_DEFINED_DEVICE_DETAIL.CONTACT
LOCATION	USER_DEFINED_DEVICE_DETAIL.LOCATION
DESCRIPTION	USER_DEFINED_DEVICE_DETAIL.DESCRIPTION
USER DEFINED VALUE1	USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE1
USER DEFINED VALUE2	USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE2
USER DEFINED VALUE3	USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE3

TABLE 83 DEVICE_INFO

Name	Source
DEVICE NODE ID	DEVICE_NODE.ID
DEVICE NODE WWN	DEVICE_NODE.WWN
DEVICE NODE TYPE	DEVICE_NODE.TYPE
DEVICE NODE SYMBOLIC NAME	DEVICE_NODE.SYMBOLIC_NAME
DEVICE_TYPE	DEVICE_NODE.DEVICE_TYPE
FDMI_HOST_NAME	DEVICE_NODE.FDMI_HOST_NAME
VENDOR	DEVICE_NODE.VENDOR
CAPABILITY_	VICE_NODE.CAPABILITY_
AG	DEVICE_NODE.AG
DEVICE PORT ID	DEVICE_PORT.ID
DEVICE PORT DOMAIN ID	DEVICE_PORT.DOMAIN_ID
DEVICE PORT WWN	DEVICE_PORT.WWN
NUMBER	DEVICE_PORT.NUMBER
PORT_ID	DEVICE_PORT.PORT_ID

TABLE 83 DEVICE_INFO (Continued)

Name	Source
DEVICE PORT TYPE	DEVICE_PORT.TYPE
DEVICE PORT SYMBOLICE NAME	DEVICE_PORT.SYMBOLIC_NAME
FC4_TYPE	DEVICE_PORT.FC4_TYPE,
IP_PORT	DEVICE_PORT.IP_PORT
HARDWARE_ADDRESS	DEVICE_PORT.HARDWARE_ADDRESS
DEVICE PORT TRUSTED	DEVICE_PORT.TRUSTED
DEVICE PORT MISSING	DEVICE_PORT.MISSING
COS	DEVICE_PORT.COS
NPV_PHYSICAL	DEVICE_PORT.NPV_PHYSICAL
SWITCH PORT ID	SWITCH_PORT.ID
SWITCH PORT WWN	SWITCH_PORT.WWN
SWITCH PORT NAME	SWITCH_PORT.NAME
SLOT_NUMBER	SWITCH_PORT.SLOT_NUMBER
PORT_NUMBER	SWITCH_PORT.PORT_NUMBER
PORT_INDEX	SWITCH_PORT.PORT_INDEX
SWITCH PORT TYPE	SWITCH_PORT.TYPE
SWITCH PORT FULL TYPE	SWITCH_PORT.FULL_TYPE
SWITCH PORT STATUS	SWITCH_PORT.STATUS
SWITCH PORT HEALTH	SWITCH_PORT.HEALTH
SPEED	SWITCH_PORT.SPEED
MAX_PORT_SPEED	SWITCH_PORT.MAX_PORT_SPEED
NPIV	SWITCH_PORT.NPIV
NPIV_CAPABLE	SWITCH_PORT.NPIV_CAPABLE
CALCULATED_STATUS	SWITCH_PORT.CALCULATED_STATUS
AREA_ID	SWITCH_PORT.AREA_ID
PHYSICAL_PORT	SWITCH_PORT.PHYSICAL_PORT
CATEGORY	SWITCH_PORT.CATEGORY
PERSISTENT_DISABLE	SWITCH_PORT.PERSISTENT_DISABLE
BLOCKED	SWITCH_PORT.BLOCKED
FCR_INTEROP_MODE	SWITCH_PORT.FCR_INTEROP_MODE
IP_ADDRESS	SWITCH_INFO.IP_ADDRESS
PHYSICAL SWITCH WWN	SWITCH_INFO.PHYSICAL_SWITCH_WWN
FIRMWARE_VERSION	SWITCH_INFO.FIRMWARE_VERSION
REACHABLE	SWITCH_INFO.REACHABLE
SYSLOG_REGISTERED	SWITCH_INFO.SYSLOG_REGISTERED
SNMP_REGISTERED	SWITCH_INFO.SNMP_REGISTERED

TABLE 83 DEVICE_INFO (Continued)

Name	Source
VIRTUAL SWITCH ID	SWITCH_INFO.ID
VIRTUAL SWITCH NAME	SWITCH_INFO.NAME
OPERATIONAL STATUS	SWITCH_INFO.OPERATIONAL_STATUS
SWITCH_MODE	SWITCH_INFO.SWITCH_MODE
VIRTUAL SWITCH WWN	SWITCH_INFO.WWN
VIRTUAL SWITCH DOMAIN ID	SWITCH_INFO.DOMAIN_ID
VIRTUAL_FABRIC_ID	SWITCH_INFO.VIRTUAL_FABRIC_ID
BASE_SWITCH	SWITCH_INFO.BASE_SWITCH
VIRTUAL SWITCH STATE	SWITCH_INFO.STATE
VIRTUAL SWITCH STATUS	SWITCH_INFO.STATUS
FABRIC ID	SWITCH_INFO.FABRIC_ID
CRYPTO_CAPABLE	SWITCH_INFO.CRYPTO_CAPABLE

TABLE 84 USER_DEEFINED_DEVICE_DETAIL

Field	Definition	Format	Size
WWN*	Device node or device port WWN.	char	23
NAME	User-assigned device name.	varchar	256
TYPE	User set device type (initiator or target).	varchar	32
IP_ADDRESS	Device IP address.	varchar	256
CONTACT	User-assigned contact.	varchar	256
LOCATION	User-assigned device location.	varchar	256
DESCRIPTION	User-assigned description.	varchar	256
USER_DEFINED_VALUE1	User-assigned arbitrary value.	varchar	256
USEER_DEFINED_VALUE2	User-assigned arbitrary value.	varchar	256
USER_DEFINED_VALUE3	User-assigned arbitrary value.	varchar	256

TABLE 85 DEVICE_NODE_INFO

Name	Source
ID	DEVICE_NODE.ID
FABRIC ID	DEVICE_NODE.FABRIC_ID
WWN	DEVICE_NODE.WWN
TYPE	DEVICE_NODE.TYPE
DEVICE TYPE	DEVICE_NODE.DEVICE_TYPE
SYMBOLIC NAME	DEVICE_NODE.SYMBOLIC_NAME
FDMI HOST NAME	DEVICE_NODE.FDMI_HOST_NAME
VENDOR	DEVICE_NODE.VENDOR

TABLE 85 DEVICE_NODE_INFO (Continued)

Name	Source
CAPABILITY	DEVICE_NODE.CAPABILITY_
TRUSTED	DEVICE_NODE.TRUSTED
CREATION TIME	DEVICE_NODE.CREATION_TIME
MISSING	DEVICE_NODE.MISSING
MISSING TIME	DEVICE_NODE.MISSING_TIME,
PROXY DEVICE	DEVICE_NODE.PROXY_DEVICE
AG	DEVICE_NODE.AG,
NAME	USER_DEFINED_DEVICE_DETAIL.NAME
USER DEFINED TYPE	USER_DEFINED_DEVICE_DETAIL.TYPE
IP ADDRESS	USER_DEFINED_DEVICE_DETAIL.IP_ADDRESS
CONTACT	USER_DEFINED_DEVICE_DETAIL.CONTACT
LOCATION	USER_DEFINED_DEVICE_DETAIL.LOCATION
DESCRIPTION	USER_DEFINED_DEVICE_DETAIL.DESCRIPTION
USER DEFINED VALUE1	USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE1
USER DEFINED VALUE2	USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE2
USER DEFINED VALUE3	USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE3

EE- Monitor

TABLE 86 EE_MONITOR_STATS

Field	Definition	Format	Size
ID*		int	
EE_MONITOR_ID	References to the ID in EE_MONITOR table.	int	
CREATION_TIME	The polling time.	timestamp	
ACTIVE_STATE	State of collection 0 = failed 1 = success	smallint	
TX	Transmit (TX) value in bytes.	double precision	
RX	Receive (RX) value in bytes.	double precision	
CRCERRORS	Number of CRC errors.	double	

TABLE 87 EE_MONITOR_STATS_30MIN

Field	Definition	Format	Size
ID*		int	
EE_MONITOR_ID		int	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
TX		double precision	
RX		double precision	
CRCERRORS		double	

TABLE 88 EE_MONITOR_STATS_2HOUR

Field	Definition	Format	Size
ID*		int	
EE_MONITOR_ID		int	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
TX		double precision	
RX		double precision	
CRCERRORS		double	

TABLE 89 EE_MONITOR

Field	Definition	Format	Size
ID*		int	
MONITOR_ID	The Number (Index) given by the switch when user creates End-End monitor on the switch.	int	
SWITCH_PORT_ID	References the ID in SWITCH_PORT table.	int	
SOURCE_PORT_ID	References the ID in DEVICE_PORT table and this is an initiator for EE monitor.	int	
DEST_PORT_ID	References the ID in DEVICE_PORT table and this is a target for EE monitor.	int	
NAME	Name of the End_End Monitor.	varchar	124
ERROR CODE	Error code returned from the switch, when enabling End-End monitor is attempted on the switch.	int	
STATUS	Status of creating the End-End monitor on the switch. It can be either failed or succeeded.	smallint	

TABLE 90 EE_MONITOR_STATS_1DAY

Field	Definition	Format	Size
ID*		int	
EE_MONITOR_ID		int	

TABLE 90 EE_MONITOR_STATS_1DAY (Continued)

Field	Definition	Format	Size
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
TX		double precision	
RX		double precision	
CRCERRORS		double	

Event/FM

TABLE 91 RECIPIENT_TYPE

Field	Definition	Format	Size
ID*		int	
TYPE	Type of the recipient (Syslog or SNMP).	varchar	20

TABLE 92 SOURCE_OBJECT_TYPE

Field	Definition	Format	Size
ID*		int	
TYPE_NAME	Type of the object to which the event applies, such as Fabric, Switch or Port.	char	64
DESCRIPTION	Description of the object	varchar	255

TABLE 93 EVENT_TYPE

Field	Definition	Format	Size
ID*		int	
TYPE_CODE	Event Type Code.	char	64
DESCRIPTION	Description of the Event Rule.	varchar	255

TABLE 94 MESSAGE_RECIPIENT

Field	Definition	Format	Size
ID*		int	
DESCRIPTION	Description about recipient.	varchar	64
IP_ADDRESS	IP Address of the recipient.	varchar	128
PORT	Port number of the recipient.	int	
RECIPIENT_TYPE_ID	Recipient Type (Syslog or SNMP).	int	

TABLE 95 EVENT_SUB_TYPE

Field	Definition	Format	Size
ID*		int	
EVENT_TYPE_ID	Unique Event Sub type ID	int	
DESCRIPTION	Description of Event Sub Type	varchar	255

TABLE 96 SNMP_CREDENTIALS

Field	Definition	Format	Size
ID*		int	
VIRTUAL_SWITCH_ID	Virtual switch ID for which this instance of the SNMP credentials apply.	int	
RECIPIENT_ID	Refers to recipient in the MESSAGE_RECIPIENT table.	int	255
PORT_NUMBER	Port number of the SNMP agent on the switch for get and set requests.	smallint	
RETRY_COUNT	Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.	smallint	
TIMEOUT	Timeout value in seconds for a get/set request to the SNMP agent. Default value is 5.	smallint	
VERSION	SNMP agent version running on the switch, as in SNMPv1 or SNMPv3.	varchar	6
READ_COMMUNITY_ STRING	The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to a device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
WRITE_COMMUNITY_ STRING	The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
USER_NAME	A human-readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
CONTEXT_NAME	Text ID associated with the user, used by SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.	varchar	128
AUTH_PROTOCOL	An indication of whether messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. Supported values are: usmNoAuthProtocol usmHMACMD5AuthProtocol usmHMACSHAAuthProtocol This is applicable if the agent is configured to operate in SNMPv3.	varchar	16

TABLE 96 SNMP_CREDENTIALS (Continued)

Field	Definition	Format	Size
AUTH_PASSWORD	The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
PRIV_PROTOCOL	An indication of whether messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. Supported values are: usmNoPrivProtocol usmDESPrivProtocol This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
PRIV_PASSWORD	The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64

TABLE 97 SYSLOG_EVENT

Field	Definition	Format	Size
ID*		int	
SWITCH_ID	Switch ID.	int	
SOURCE_NAME	Source Name from which the event originated.	varchar	32
SOURCE_ADDR	IP Address from which the event originated.	varchar	32
EVENT_SOURCE	Source from which the event is generated.	varchar	32
STATUS	Status of the event.	varchar	32
PRIORITY	Priority of the event. Default priority is 7.	int	
EVENT_NUMBER	Sequence number of the event.	int	
EVENT_COUNT	Number of occurrences of the event.	int	
AUDIT	Audit file of the syslog message.	varchar	10
FIRST_OCCURENCE_ SWITCH_TIME	First occurrence switch time.	timestamp	
LAST_OCCURENCE_ SWITCH_TIME	Last occurrence switch time.	timestamp	
FIRST_OCCURENCE_ HOST_TIME	Last occurrence switch time.	timestamp	
LAST_OCCURENCE_HOST_ TIME	Last occurrence host time.	timestamp	
MODULE	Module of the event.	varchar	10
MESSAGE_ID	Message ID of the event.	varchar	20
DESCRIPTION	Description of the event.	varchar	512
PROBABLE_CAUSE	Probable root cause of the event.	varchar	512
RECOMMENDED_ACTION	Recommended action for the event.	varchar	512
CONTRIBUTORS	Contributors of the syslog event.	varchar	512

TABLE 98 EVENT

Field	Definition	Format	Size
ID*		int	
SWITCH_ID	ID of the switch.	int	
PARENT_ID	ID of the Parent.	int	255
SOURCE_NAME	Name of the source from which the event originated.	varchar	32
SOURCE_ADDR	IP Address of the source from which the event originated.	varchar	50
EVENT_SOURCE	Source from which the event is generated.	varchar	32
SINK_SOURCE	Sink Source of the event (Syslog/SNMP Trap/errlog/Application).	varchar	32
STATUS	Status of the event (Down/Marginal/Healthy).	varchar	32
PRIORITY	Event priority, by default the value will be 7 (Unknown).	int	
EVENT_NUMBER	Sequence number of the event. A Sequence number is received from certain events, but for others it defaults to 0.	int	
EVENT_COUNT	Number of occurrences of the event.	int	
AUDIT	Flag to indicate if the event is audited.	varchar	10
FIRST_OCCURENCE_ SWITCH_TIME	First occurrence switch time.	timestamp	
LAST_OCCURENCE_ SWITCH_TIME	Last occurrence switch time.	timestamp	
FIRST_OCCURENCE_HOST_ TIME	First occurrence host time; this is set to GMT time.	timestamp	
LAST_OCCURENCE_HOST_ TIME	Last occurrence host time; this is set to GMT time.	timestamp	
MODULE	Module from which the event is generated.	varchar	20
MESSAGE_ID	Unique message ID of the event.	varchar	20
DESCRIPTION	Description of the event.	varchar	512
RESOLVED	Resolution status of the event.	smallint	
ACKNOWLEDGED	Acknowledgement status of the event.	smallint	
ACKED_BY	User who acknowledged the event	varchar	80
ACKED_TIME	Time at which the event is acknowledged	timestamp	
PORBABLE_CAUSE	Probable root cause of the event	varchar	512
RECOMMENDED_ACTION	Recommended action for the event	varchar	512
CONTRIBUTORS	Contributors of the event	varchar	512
SOURCE_OBJECT_ID	Source Object ID	int	
SOURCE_OBJECT_TYPE_ID	Source Object type	int	
EVENT_TYPE_ID	Event Type ID of the event	int	
EVENT_SUB_TYPE_ID	Sub Type ID of the event	int	

TABLE 98 EVENT (Continued)

Field	Definition	Format	Size
EVENT_CATEGORY	Category of the event	varchar	64
DISCOVERY_TYPE	Discovery type of the product	varchar	64
MANAGEMENT_LINK	Management link status	varchar	255
OPERATIONAL_STATUS	Operational Status of the switch from which the event is triggered	varchar	255
NODE_WWN	WWN of the node from which the event is triggered	varchar	23
PORT_WWN	WWN of the port from which the event is triggered	varchar	23
NODE_NAME	Node Name from which the event is triggered	varchar	255
PORT_NAME	Port Name from which the event is triggered	varchar	255
RESOLVED_TIME	Time at which the event is resolved	timestamp	
FRU_CODE	FRU Code used for call home	int	
REASON_CODE	Event Reason code to identify the event uniquely	int	
FRU_POSITION	Failed FRU position in case of FRU failure, 0 otherwise	int	
CALL_HOME	Call Home status of the Event. 1 = call home event. 0 = not a call home event.	smallint	
OID	Object Identifier of the SNMP Trap Event. For other events, this column will be blank	varchar	50

TABLE 99 RAS_LOG

Field	Definition	Format	Size
MSG_ID*	Message ID of the event.	varchar	15
MODULE_ID	Module ID of the event.	varchar	10
SEVERITY	Severity of the event.	varchar	10
CAUSE	Probable root cause for the event.	varchar	4096
ACTION	Recommended action for the event.	varchar	4096
OLD_MSG_ID	Old message ID.	varchar	45

TABLE 100 EVENT_NOTIFICATION

Field	Definition	Format	Size
ID*		int	
STATUS	Status of Event Notification. value will be 0 if disabled, 1 otherwise.	smallint	
SERVER_NAME	E-mail (SMTP) server name.	varchar	256
REPLY_ADDRESS	Reply E-mail address.	varchar	50
SEND_ADDRESS	E-mail address for which a Test E-mail notification is to be sent.	varchar	512
SMTP_PORT	SMTP Port number.	int	

TABLE 100 EVENT_NOTIFICATION (Continued)

Field	Definition	Format	Size
USER_NAME	User name for authentication.	varchar	256
PASSWORD	Password for authentication.	varchar	256
NOTIFICATION_INTERVAL	Time interval between successive event notifications.	int	
NOTIFICATION_UNIT	Time interval Unit: 0 = Seconds 1 = Minutes 2 = Hours	smallint	
TEST_OPTION	Time interval Unit: 0 = Send test to configured e-mail address. 1 = Send test to all enabled users.	smallint	

TABLE 101 EVENT_RULE

Field	Definition	Format	Size
ID*		int	
NAME	Name of the Event Rule.	varchar	255
TYPE	Event Rule Type: 0 = ISL Offline 1 = PM Threshold crossed 2 = Security Violation 4 = Event	int	
DESCRIPTION	Description about the Event Rule.	varchar	512
OPERATOR1	AND operator used to append the rule.	varchar	12
EVENT_TYPE_ID	The Selected Event type ID from the Event type combo box.	int	
OPERATOR2	AND operator used to append the rule.	varchar	12
MESSAGE_ID	Message ID provided by the user.	varchar	20
OPERATOR3	AND operator used to append the rule.	varchar	12
IP_ADDRESS	Source IP Address.	varchar	32
OPERATOR4	AND operator used to append the rule.	varchar	12
WWN	Source WWN.	varchar	255
OPERATOR5	AND operator used to append the rule.	varchar	12
COUNT	Count of the specified event.	int	
OPERATOR6	AND operator used to append the rule.	varchar	12
DURATION	Duration of the specified event.	bigint	
STATE	State of the rule: 0 = Disabled 1 = Enabled	smallint	
SEVERITY_LEVEL	Event severity level.	int	
SOURCE_NAME	Name of the source.	varchar	255
DESCRIPTION_CONTAINS	Description pattern about the rule.	varchar	255

TABLE 101 EVENT_RULE (Continued)

Field	Definition	Format	Size
LAST_MODIFIED_TIME	Rules last edited time.	timestamp	
SELECTED_TIME_UNIT	Timestamp unit of the selected rule: 0 = second 1 = Minutes 2 = Hours	smallint	

TABLE 102 EVENT_RULE_ACTION

Field	Definition	Format	Size
ID*		int	
RULE_ID	The rule ID present in the Event_Rule Table.	int	
NAME	Name of the Event Rule Action: Launch Script = for launch script Send E-mail = for send e-mail Raise Event = for broadcast message	varchar	255
TYPE	Name of the action: script = for Launch Script e-mail = for E-mail message = for Broadcast message	varchar	30
FIELD1	Data for the selected action.	varchar	512
FIELD2	Data for the selected action.	varchar	512
FIELD3	Data for the selected action.	varchar	512
FIELD4	Data for the selected action.	varchar	512
STATE	State of the Action: 0 = Action Disabled 1 = Action Enabled	smallint	

Fabric

TABLE 103 SAN

Field	Definition	Format	Size
ID*		int	
NAME	Name of this SAN.	varchar	256
CONTACT	Contact person for this SAN.	varchar	256
LOCATION	Location of this SAN.	varchar	256
DESCRIPTION	Description.	varchar	256
STATS_COLLECTION	1 = statistics collection is enabled; otherwise, 0.	smallint	
CREATION_TIME	time at which this record was created.	timestamp	
LAST_UPDATE_TIME	time when this was last updated.	timestamp	

TABLE 104 FABRIC

Field	Definition	Format	Size
ID*		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256
TYPE	Type of fabric: 0 = legacy fabric 1 = base fabric 2 = logical fabric	smallint	
SECURE	1 = it is a secured fabric.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone configuration which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

TABLE 105 FABRIC_INFO

Name	Source
ID	FABRIC.ID
SAN_ID	FABRIC.SAN_ID
SEED_SWITCH_WWN	FABRIC.SEED_SWITCH_WWN
NAME	FABRIC.NAME
ACTIVE_ZONESET_NAME	FABRIC.ACTIVE_ZONESET_NAME

TABLE 105 FABRIC_INFO (Continued)

Name	Source
MANAGEMENT_STATE	FABRIC.MANAGEMENT_STATE
LAST_FABRIC_CHANGED	FABRIC.LAST_FABRIC_CHANGED
SECURE	FABRIC.SECURE
AD_ENVIRONMENT	FABRIC.AD_ENVIRONMENT
MANAGED	FABRIC.MANAGED
CONTACT	FABRIC.CONTACT
LOCATION	FABRIC.LOCATION
DESCRIPTION	FABRIC.DESCRIPTION
CREATION_TIME	FABRIC.CREATION_TIME
LAST_SCAN_TIME	FABRIC.LAST_SCAN_TIME
LAST_UPDATE_TIME	FABRIC.LAST_UPDATE_TIME
TRACK_CHANGES	FABRIC.TRACK_CHANGES
TYPE	FABRIC.TYPE
USER_DEFINED_VALUE_1	FABRIC.USER_DEFINED_VALUE_1
USER_DEFINED_VALUE_2	FABRIC.USER_DEFINED_VALUE_2
USER_DEFINED_VALUE_3	FABRIC.USER_DEFINED_VALUE_3
ID	VIRTUAL_SWITCH.ID
SEED SWITCH IP ADDRESS	CORE_SWITCH.IP_ADDRESS
SWITCH COUNT	FABRIC_MEMBER.FABRIC_ID = FABRIC.ID

TABLE 106 FABRIC_MEMBER

Field	Definition	Format	Size
FABRIC_ID*	Fabric ID, foreign key to FABRIC table.	INT	
VIRTUAL_SWITCH_ID*	ID of the virtual switch which is a member of this fabric, foreign key to VIRTUAL_SWITCH table.	INT	
TRUSTED	1 = the switch is a trusted member of the fabric. Either found in the initial discovery or user subsequently entrusted the switch by user action.	SMALLINT	
CREATION_TIME	When the switch became a member.	TIMESTAMP	
MISSING	1 = it is missing from the fabric.	SMALLINT	
MISSING_TIME	When it is missed from the fabric; null if the member is entrusted.	TIMESTAMP	

FC Port Stats

TABLE 107 FC_PORT_STATS

Field	Definition	Format	Size
ID*		int	
SWITCH_ID	References the ID in CORE_SWITCH table.	int	
PORT_ID	References the ID in SWITCH_PORT table.	int	
TX	Transmission (TX) value in bytes.	double	
RX	Receive (RX) value in bytes.	double	
TX_UTILIZATION	Transmit utilization value in percentage.	double	
RX_UTILIZATION	Receive utilization value in percentage.	double‘	
CREATION_TIME	The polling time.	timestamp	
ACTIVE_STATE	State of collection: 0 = failed 1 = success	smallint	
LINKFAILURES	Number of link failures.	double	
TXLINKRESETS	Number of transmit link failures.	double	
RXLINKRESETS	Number of receive link failures.	double	
SYNCLOSSES	Number of sync losses.	double	
SIGNALLOSSES	Number of signal losses.	double	
SEQUENCEERRORS	Number of sequence errors.	double	
INVALIDTRANSMISSIONS	Number of invalid transmission errors.	double	
CRCERRORS	Number of CRC errors.	double	

TABLE 108 FC_PORT_STATS_30MIN

Field	Definition	Format	Size
ID*		int	
SWITCH_ID		int	
PORT_ID		int	
TX		double	
RX		double	
TX_UTILIZATION		double	
RX_UTILIZATION		double‘	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
LINKFAILURES		double	
TXLINKRESETS		double	
RXLINKRESETS		double	
SYNCLOSSES		double	

TABLE 108 FC_PORT_STATS_30MIN (Continued)

Field	Definition	Format	Size
SIGNALLOSSES		double	
SEQUENCEERRORS		double	
INVALIDTRANSMISSIONS		double	
CRCERRORS		double	
DATA_GAPS_IN5MIN		smallint	

TABLE 109 FC_PORT_STATS_2HOUR

Field	Definition	Format	Size
ID*		int	
SWITCH_ID		int	
PORT_ID		int	
TX		double	
RX		double	
TX_UTILIZATION		double	
RX_UTILIZATION		double‘	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
LINKFAILURES		double	
TXLINKRESETS		double	
RXLINKRESETS		double	
SYNCLOSSES		double	
SIGNALLOSSES		double	
SEQUENCEERRORS		double	
INVALIDTRANSMISSIONS		double	
CRCERRORS		double	
DATA_GAPS_IN5MIN		smallint	
DATA_GAPS_IN30MIN		smallint	

TABLE 110 FC_PORT_STATS_1DAY

Field	Definition	Format	Size
ID*		int	
SWITCH_ID		int	
PORT_ID		int	
TX		double	
RX		double	
TX_UTILIZATION		double	

TABLE 110 FC_PORT_STATS_1DAY (Continued)

Field	Definition	Format	Size
RX_UTILIZATION		double‘	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
LINKFAILURES		double	
TXLINKRESETS		double	
RXLINKRESETS		double	
SYNCLOSSES		double	
SIGNALLOSSES		double	
SEQUENCEERRORS		double	
INVALIDTRANSMISSIONS		double	
CRCERRORS		double	
DATA_GAPS_IN5MIN		smallint	
DATA_GAPS_IN30MIN		smallint	
DATA_GAPS_IN2HOUR		smallint	

FCIP

TABLE 111 FCIP_TUNNEL

Field	Definition	Format	Size
ID*		int	
ETHERNET_PORT_ID	GigE Port ID on which the tunnel is created.	int	
TUNNEL_ID	Tunnel ID for that GigE Port.	smallint	
VLAN_TAG	VLAN Tag on the tunnel (if present).	int	
SOURCE_IP	Source IP on which the tunnel is created.	char	64
DEST_IP	Destination IP on the other end of tunnel.	char	64
LOCAL_WWN	Local port WWN for the tunnel.	char	23
REMOTE_WWN_RESTRICT	Remote Port WWN for the tunnel.	char	23
COMMUNICATION_RATE	Bandwidth specified for the tunnel.	double	
MIN_RETRANSMIT_TIME	FCIP Tunnel Parameter.	int	
SELECTIVE_ACK_ENABLED	FCIP Tunnel Parameter.	smallint	
KEEP_ALIVE_TIMEOUT	FCIP Tunnel Parameter.	int	
MAX_RETRNASMISSION	FCIP Tunnel Parameter.	int	
PATH_MTU_DISCOVERY_ ENABLED	FCIP Tunnel Parameter.	smallint	
WAN_TOV_ENABLED	FCIP Tunnel Parameter.	smallint	
TUNNEL_STATUS	Tunnel Status (Active/Inactive).	int	

TABLE 112 FCIP_TUNNEL_INFO

Name	Source
ID	FCIP_TUNNEL.ID
ETHERNET_PORT_ID	FCIP_TUNNEL.ETHERNET_PORT_ID
TUNNEL_ID	FCIP_TUNNEL.TUNNEL_ID
VLAN_TAG	FCIP_TUNNEL.VLAN_TAG
SOURCE_IP	FCIP_TUNNEL.SOURCE_IP
DEST_IP	FCIP_TUNNEL.DEST_IP
LOCAL_WWN	FCIP_TUNNEL.LOCAL_WWN
REMOTE_WWN_RESTRICT	FCIP_TUNNEL.REMOTE_WWN_RESTRICT
COMMUNICATION_RATE	FCIP_TUNNEL.COMMUNICATION_RATE
MIN_RETRANSMIT_TIME	FCIP_TUNNEL.MIN_RETRANSMIT_TIME
SELECTIVE_ACK_ENABLED	FCIP_TUNNEL.SELECTIVE_ACK_ENABLED
KEEP_ALIVE_TIMEOUT	FCIP_TUNNEL.KEEP_ALIVE_TIMEOUT
MAX_RETRNASMISSION	FCIP_TUNNEL.MAX_RETRANSMISSION
PATH_MTU_DISCOVERY_ENABLED	FCIP_TUNNEL.PATH_MTU_DISCOVERY_ENABLED

TABLE 112 FCIP_TUNNEL_INFO (Continued)

Name	Source
WAN_TOV_ENABLED	FCIP_TUNNEL.WAN_TOV_ENABLED
TUNNEL_STATUS	FCIP_TUNNEL.TUNNEL_STATUS
COMPRESSION_ENABLED	FCIP_TUNNEL_DETAILS.COMPRESSION_ENABLED
TURBO_WRITE_ENALBED	FCIP_TUNNEL_DETAILS.TURBO_WRITE_ENABLED
TAPE_ACCELERATION_ENABLED	FCIP_TUNNEL_DETAILS.TAPE_ACCELERATION_ENABLED
IKE_POLICY_NUM	FCIP_TUNNEL_DETAILS.IKE_POLICY_NUM
IPSEC_POLICY_NUM	FCIP_TUNNEL_DETAILS.IPSEC_POLICY_NUM
PRESHARED_KEY	FCIP_TUNNEL_DETAILS.PRESHARED_KEY
FICON_TAPE_READ_BLOCK_ID_ ENABLED	FCIP_TUNNEL_DETAILS.FICON_TAPE_READ_BLOCK_ID_ENABLED
FICON_TIN_TIR_EMULATION_E NABLED	FCIP_TUNNEL_DETAILS.FICON_TIN_TIR_EMULATION_ENABLED
FICON_DEVICE_LEVEL_ACK_EM ULATION_ENABLED	FCIP_TUNNEL_DETAILS.FICON_DEVICE_LEVEL_ACK_EMULATION_ENABLED
FICON_TAPE_WRITE_MAX_PIPE	FCIP_TUNNEL_DETAILS.FICON_TAPE_WRITE_MAX_PIPE
FICON_TAPE_READ_MAX_PIPE	FCIP_TUNNEL_DETAILS.FICON_TAPE_READ_MAX_PIPE
FICON_TAPE_WRITE_MAX_OPS	FCIP_TUNNEL_DETAILS.FICON_TAPE_WRITE_MAX_OPS
FICON_TAPE_READ_MAX_OPS	FCIP_TUNNEL_DETAILS.FICON_TAPE_READ_MAX_OPS
FICON_TAPE_WRITE_TIMER	FCIP_TUNNEL_DETAILS.FICON_TAPE_WRITE_TIMER
FICON_TAPE_MAX_WRITE_CHAI N	FCIP_TUNNEL_DETAILS.FICON_TAPE_MAX_WRITE_CHAIN
FICON_OXID_BASE	FCIP_TUNNEL_DETAILS.FICON_OXID_BASE
FICON_XRC_EMULATION_ENAB LED	FCIP_TUNNEL_DETAILS.FICON_XRC_EMULATION_ENABLED
FICON_TAPE_WRITE_EMULATIO N_ENABLED	FCIP_TUNNEL_DETAILS.FICON_TAPE_WRITE_EMULATION_ENABLED
FICON_TAPE_READ_EMULATIO N_ENABLED	FCIP_TUNNEL_DETAILS.FICON_TAPE_READ_EMULATION_ENABLED
FICON_DEBUG__FLAGS	FCIP_TUNNEL_DETAILS.FICON_DEBUG_FLAGS
SLOT_NUMBER	GIGE_PORT.SLOT_NUMBER
SWITCH PORT ID	GIGE_PORT.PORT_NUMBER
ID	SWITCH_PORT.ID
VIRTUAL_SWITCH_ID	SWITCH_PORT.VIRTUAL_SWITCH_ID
USER_PORT_NUMBER	SWITCH_PORT.USER_PORT_NUMBER
VIRTUAL PORT WWN	FCIP_PORT_TUNNEL_MAP.TUNNEL_ID = FCIP_TUNNEL.ID and FCIP_PORT_TUNNEL_MAP.SWITCHPORT_ID = PORT.ID) VIRTUAL_PORT_WWN

TABLE 112 FCIP_TUNNEL_INFO (Continued)

Name	Source
REMOTE PORT WWN	FCIP_PORT_TUNNEL_MAP.TUNNEL_ID = FCIP_TUNNEL.ID and FCIP_PORT_TUNNEL_MAP.SWITCHPORT_ID = PORT.ID) REMOTE_PORT_WWN
REMOTE NODE WWN	FCIP_PORT_TUNNEL_MAP.TUNNEL_ID = FCIP_TUNNEL.ID and FCIP_PORT_TUNNEL_MAP.SWITCHPORT_ID = PORT.ID) REMOTE_NODE_WWN

TABLE 113 FCIP_PORT_TUNNEL_MAP

Field	Definition	Format	Size
SWITCHPORT_ID*	Switch Port ID.	int	
TUNNEL_ID*	FCIP Tunnel ID.	int	

TABLE 114 FCIP_TUNNEL_DETAILS

Field	Definition	Format	Size
TUNNEL_ID*	Tunnel ID for that GigE Port.	int	
COMPRESSION_ENABLED	Whether Compression is enabled on that tunnel.	smallint	
TURBO_WRITE_ENABLED	Whether TurboWrite is enabled on that tunnel.	smallint	
TAPE_ACCELERATION_ ENABLED	Whether TapeAccelaration is enabled on that tunnel.	smallint	
IKE_POLICY_NUM	The IKE Policy on the tunnel.	int	
IPSEC_POLICY_NUM	The IPSEC Policy on the tunnel.	int	
PRESHARED_KEY	The Preshared Key on the tunnel.	char	32
FICON_TAPE_READ_BLOCK _ID_ENABLED	Whether Ficon_Tape_Read_Block is enabled on that tunnel.	smallint	
FICON_TIN_TIR_ EMULATION_ENABLED	Whether Ficon_Tin_Tir_Emulation is enabled on that tunnel.	smallint	
FICON_DEVICE_LEVEL_ ACK_EMULATION_ENABLED	Whether Device_Level_Ack_Emulation is enabled on that tunnel.	smallint	
FICON_TAPE_WRITE_MAX_ PIPE	The value for this on the tunnel.	int	
FICON_TAPE_READ_MAX_ PIPE	The value for this on the tunnel.	int	
FICON_TAPE_WRITE_MAX_ OPS	The value for this on the tunnel.	int	
FICON_TAPE_READ_MAX_ OPS	The value for this on the tunnel.	int	
FICON_TAPE_WRITE_TIMER	The value for this on the tunnel.	int	
FICON_TAPE_MAX_WRITE_ CHAIN	The value for this on the tunnel.	int	
FICON_OXID_BASE	The value for this on the tunnel.	int	
FICON_XRC_EMULATION_ ENABLED	Whether XRC Emulation is enabled on the tunnel.	smallint	

TABLE 114 FCIP_TUNNEL_DETAILS (Continued)

Field	Definition	Format	Size
FICON_TAPE_WRITE_ EMULATION_ENABLED	Whether this is enabled on that tunnel.	smallint	
FICON_TAPE_READ_ EMULATION_ENABLED	Whether this is enabled on that tunnel.	smallint	
FICON_DEBUG__FLAGS	FICON_DEBUG_FLAGS for that particular tunnel.	double	

FCIP Tunnel Stats

TABLE 115 FCIP_TUNNEL_STATS

Field	Definition	Format	Size
ID*		int	
TUNNEL_DBID	References the ID in FCIP_TUNNEL table.	int	
SWITCH ID	References the ID in CORE_SWITCH table.	int	
CREATION TIME	The polling time.	timestamp	
TX	Transmit (TX) value in bytes.	double precision	
RX	Receive (RX) value in bytes.	double precision	
TX_UTILIZATION	Transmit utilization value in percentage.	double precision	
RX_UTILIZATION	Receive utilization value in percentage.	double precision	
DROPPED PACKETS	The number of dropped packets.	double precision	
COMPRESSION	The compression value.	double precision	
LATENCY	The latency value.	double precision	
LINK_RETRANSMITS	The number of link retransmits.	double precision	
ACTIVE_STATE	State of collection: 0 = failed 1 = success	smallint	

TABLE 116 FCIP_TUNNEL_STATS_30MIN

Field	Definition	Format	Size
ID*		int	
TUNNEL_DBID		int	
SWITCH ID		int	
CREATION TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	

TABLE 116 FCIP_TUNNEL_STATS_30MIN (Continued)

Field	Definition	Format	Size
DROPPED PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	
LINK_RETRANSMITS		double precision	
ACTIVE_STATE		smallint	

TABLE 117 FCIP_TUNNEL_STATS_2HOUR

Field	Definition	Format	Size
ID*		int	
TUNNEL_DBID		int	
SWITCH ID		int	
CREATION TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	
LINK_RETRANSMITS		double precision	
ACTIVE_STATE		smallint	

TABLE 118 FCIP_TUNNEL_STATS_1DAY

Field	Definition	Format	Size
ID*		int	
TUNNEL_DBID		int	
SWITCH ID		int	
CREATION TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	

TABLE 118 FCIP_TUNNEL_STATS_1DAY (Continued)

Field	Definition	Format	Size
LINK_RETRANSMITS		double precision	
ACTIVE_STATE		smallint	

TABLE 119 FCIP_TUNNEL

Field	Definition	Format	Size
ID*		int	
ETHERNET_PORT_ID	GigE Port ID on which the tunnel is created.	int	
TUNNEL_ID	Tunnel ID for that GigE Port.	smallint	
VLAN_TAG	VLAN Tag on the tunnel (if present).	int	
SOURCE_IP	Source IP on which the tunnel is created.	char	64
DEST_IP	Destination IP on the other end of tunnel.	char	64
LOCAL_WWN	Local port WWN for the tunnel.	char	23
REMOTE_WWN_RESTRICT	Remote Port WWN for the tunnel.	char	23
COMMUNICATION_RATE	Bandwidth specified for the tunnel.	double	
MIN_RETRANSMIT_TIME	FCIP Tunnel Parameter.	int	
SELECTIVE_ACK_ENABLED	FCIP Tunnel Parameter.	smallint	
KEEP_ALIVE_TIMEOUT	FCIP Tunnel Parameter.	int	
MAX_RETRANSMISSION	FCIP Tunnel Parameter.	int	
PATH_MTU_DISCOVERY_ ENABLED	FCIP Tunnel Parameter.	smallint	
WAN_TOV_ENABLED	FCIP Tunnel Parameter.	smallint	
TUNNEL_STATUS	Tunnel Status (Active/Inactive).	int	

GigE Port Stats

TABLE 120 GIGE_PORT_STATS

Field	Definition	Format	Size
ID*		int	
SWITCH ID	References the ID in CORE_SWITCH table.	int	
PORT_ID	References the ID in SWITCH_PORT table.	int	
CREATION TIME	The polling time.	timestamp	
TX	Transmit (TX) value in bytes.	double precision	
RX	Receive (RX) value in bytes.	double precision	
TX_UTILIZATION	Transmit utilization (TX%) value in percentage.	double precision	
RX_UTILIZATION	Receive utilization (RX%) value in percentage.	double precision	

TABLE 120 GIGE_PORT_STATS (Continued)

Field	Definition	Format	Size
DROPPED PACKETS	Number of dropped packets.	double precision	
COMPRESSION	The compression value.	double precision	
LATENCY	The latency value.	double precision	
BANDWIDTH	The bandwidth value.	double precision	

TABLE 121 GIGE_PORT_STATS_30MIN

Field	Definition	Format	Size
ID*		int	
SWITCH ID		int	
PORT_ID		int	
CREATION TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	
BANDWIDTH		double precision	

TABLE 122 GIGE_PORT_STATS_2HOUR

Field	Definition	Format	Size
ID*		int	
SWITCH ID		int	
PORT_ID		int	
CREATION TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	
BANDWIDTH		double precision	

TABLE 123 GIGE_PORT_STATS_1DAY

Field	Definition	Format	Size
ID*		int	
SWITCH ID		int	
PORT_ID		int	
CREATION TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	
BANDWIDTH		double precision	

ISL

TABLE 124 ISL_INFO

Name	Source
ID	ISL.ID
FABRIC_ID	ISL.FABRIC_ID
COST	ISL.COST
TYPE	ISL.TYPE
SOURCE_DOAMIN_ID	ISL.SOURCE_DOMAIN_ID
SOURCE PORT NUMBER	ISL.SOURCE_PORT_NUMBER
SOURCE SWITCH ID	SOURCE_VIRTUAL_SWITCH.ID
SOURCE SWITCH NAME	SOURCE_VIRTUAL_SWITCH.NAME
SOURCE SWITCH PORT ID	SOURCE_SWITCH_PORT.ID
SOURCE SWITCH PORT WWN	SOURCE_SWITCH_PORT.WWN
DEST DOMAIN ID	ISL.DEST_DOMAIN_ID
DEST PORT NUMBER	ISL.DEST_PORT_NUMBER
DEST SWITCH ID	DEST_VIRTUAL_SWITCH.ID
DEST SWITCH NAME	DEST_VIRTUAL_SWITCH.NAME
DEST SWITCH PORT ID	DEST_SWITCH_PORT.ID
DEST SWITCH PORT WWN	DEST_SWITCH_PORT.WWN

TABLE 125 ISL_TRUNK_INFO

Name	Source
ID	ISL_TRUNK_GROUP.ID
COST	ISL_INFO.COST
TYPE	ISL_INFO.TYPE
SOURCE PORT NUMBER	ISL_INFO.SOURCE_PORT_NUMBER
SOURCE SWITCH ID	ISL_INFO.SOURCE_SWITCH_ID
SOURCE SWITCH IP ADDRESS	SOURCE_CORE_SWITCH.IP_ADDRESS
SOURCE SWITCH WWN	SOURCE_VIRTUAL_SWITCH.WWN
MASTER PORT	ISL_INFO.SOURCE_DOMAIN_ID
SOURCE SWITCH NAME	ISL_INFO.SOURCE_SWITCH_NAME
SOURCE SWITCH PORT ID	ISL_INFO.SOURCE_SWITCH_PORT_ID
DEST PORT NUMBER	ISL_INFO.DEST_PORT_NUMBER
DEST SWITCH ID	ISL_INFO.DEST_SWITCH_ID
DEST SWITCH IP ADDRESS	DEST_CORE_SWITCH.IP_ADDRESS
DEST SWITCH WWN	DEST_VIRTUAL_SWITCH.WWN
DEST SWITCH PORT WWN	ISL_INFO.SOURCE_SWITCH_PORT_WWN
SOURCE SWITCH PORT WWN	
REMOTE MASTER PORT	
DEST SWITCH NAME	ISL_INFO.DEST_SWITCH_NAME
DEST SWITCH PORT ID	ISL_INFO.DEST_SWITCH_PORT_ID

TABLE 126 ISL

Field	Definition	Format	Size
ID*		int	
FABRIC_ID	Fabric DB ID.	int	
SOURCE_DOMAIN_ID	Source domain ID.	int	
SOURCE_PORT_NUMBER	Source port number.	smallint	
DEST_DOMAIN_ID	Destination domain ID.	int	
DEST_PORT_NUMBER	Destination port number.	smallint	
COST	The cost of the link.	int	
TYPE	The type of link.	smallint	
TRUSTED	1 = ISL is trusted 0 = ISL is not trusted	smallint	
CREATION_TIME	Time at which this record was created.	timestamp	
MISSING	1 = ISL is missing 0 = ISL is not missing	smallint	
MISSING_TIME	Time at which ISL went missing.	timestamp	

TABLE 127 FABRIC

Field	Definition	Format	Size
ID*		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256
TYPE	Type of fabric: 0 = legacy fabric 1 = base fabric 2 = logical fabric	smallint	
SECURE	1 = it is a secured fabric.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone set which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

TABLE 128 ISL_TRUNK_MEMBER

Field	Definition	Format	Size
GROUP_ID*	ISL_TRUNK_GROUP DB ID.	int	
PORT_NUMBER*	Port number of member port.	smallint	

TABLE 129 ISL_TRUNK_GROUP

Field	Definition	Format	Size
ID*		int	
VIRTUAL_SWITCH_ID	Virtual switch DB ID.	int	
MASTER_USER_PORT	Port number of master port.	smallint	

License

TABLE 130 LICENSE_FEATURE_MAP

Field	Definition	Format	Size
LICENSE_ID*	Foreign Key (SWITCH_LICENSE.ID) and is part of the primary key.	integer	
FEATURE_ID*	Foreign Key (LICENSED_FEATURE.ID) and is part of the primary.	integer	

TABLE 131 LICENSED_FEATURE

Field	Definition	Format	Size
ID*		int	
NAME	License feature name, a short text description.	varchar	64
DESCRIPTION	Optional detailed description about the license feature.	varchar	256

TABLE 132 SWITCH_LICENSE

Field	Definition	Format	Size
ID*		int	
CORE_SWITCH_ID	Refers to the entry in the CORE_SWITCH table.	int	
LICENSE_KEY	Stores the license key obtained from the switch.	varchar	256

TABLE 133 CORE_SWITCH

Field	Definition	Format	Size
ID*		int	

Meta SAN

TABLE 134 LSAN_DEVICE

Field	Definition	Format	Size
ID*		int	
BB_FABRIC_ID	Backbone fabric DB ID.	int	
FCR_FABRIC_ID	FID assigned to edge fabric.	int	
DEVICE_PORT_WWN	Device port WWN of physical device.	char	23
PHYSICAL_PID	PID of physical device.	char	6

TABLE 135 LSAN_PROXY_DEVICE

Field	Definition	Format	Size
FCR_FABRIC_ID*	FID assigned to edge fabric	int	
PROXY_PID*	Proxy device PID	char	6
STATE	State of the device	varchar	128
LSAN_DEVICE_ID*	LSAN_DEVICE record reference	int	

TABLE 136 FCR_ROUTE

Field	Definition	Format	Size
ID*		INT	
BB_FABRIC_ID	Backbone fabric DB ID.	INT	
FCR_FABRIC_ID	FID assigned to edge fabric.	INT	
SWITCH_WWN	WWN of the router switch.	VARCHAR	128
NR_PORT_ID	Route parameter.	INT	
FCRP_COST	Route parameter.	INT	
EX_PORT_WWN	Ex_port WWN.	VARCHAR	128

TABLE 137 FABRIC

Field	Definition	Format	Size
ID*		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256

TABLE 137 FABRIC (Continued)

Field	Definition	Format	Size
TYPE	Type of fabric: 0 = legacy fabric 1 = base fabric 2 = logical fabric	smallint	
SECURE	1 = it is a secured fabric.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone set which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

TABLE 138 IFL

Field	Definition	Format	Size
ID*		int	
EDGE_FABRIC_ID	Edge Fabric ID.	int	
EDGE_PORT_WWN	Edge Fabric Port WWN.	varchar	128
BB_FABRIC_ID	Backbone Fabric ID.	int	
BB_PORT_WWN	Backbone Fabric Port WWN.	varchar	128
BB_RA_TOV	Backbone RA TOV.	int	
BB_ED_TOV	Backbone ED TOV.	int	
BB_PID_FORMAT	Backbone PID Format.	smallint	

TABLE 139 IFL_INFO

Name	Source
ID	IFL.ID
EDGE_FABRIC_ID	IFL.EDGE_FABRIC_ID
FCR SWITCH ID	FCR_PORT.VIRTUAL_SWITCH_ID
EDGE_PORT_WWN	IFL.EDGE_PORT_WWN
BB_FABRIC_ID	IFL.BB_FABRIC_ID
BB_PORT_WWN	IFL.BB_PORT_WWN
BB_RA_TOV	IFL.BB_RA_TOV
BB_ED_TOV	IFL.BB_ED_TOV
BB_PID_FORMAT	IFL.BB_PID_FORMAT
EDGE SWITCH ID	SWITCH_PORT.VIRTUAL_SWITCH_ID
EDGE PORT ID	SWITCH_PORT.ID
EDGE PORT NUMBER	SWITCH_PORT.USER_PORT_NUMBER
EDGE PORT TYPE	SWITCH_PORT.TYPE

Network

TABLE 140 IP_INTERFACE

Field	Definition	Format	Size
ID*		int	
ETHERNET_PORT_ID	GigE Port ID.	int	
IP_ADDRESS	IP address on the Ip_interface.	varchar	64
NET_MASK	Subnet mask for the interface.	varchar	64
MTU_SIZE	MTU Size for that interface.	int	
CHECKSUM	Check Sum.	varchar	64

TABLE 141 IP_ROUTE

Field	Definition	Format	Size
ID*		int	
ETHERNET_PORT_ID	GigE Port ID.	int	
PORT_NUMBER	Port Number related to the GigE Port.	int	
SLOT_NUMBER	Slot Number related to the GigE Port.	int	
NET_MASK	Subnet Mask for the Route.	varchar	64
GATEWAY	Gateway for the Route.	varchar	64
IP_ADDRESS	IP Address created after "&" operation of gateway.	varchar	64
METRIC	Metric.	int	

TABLE 141 IP_ROUTE (Continued)

Field	Definition	Format	Size
FLAG	Flag.	int	
CHECKSUM	Check Sum.	varchar	64

Others

TABLE 142 SYSTEM_PROPERTY

Field	Definition	Format	Size
NAME*	The name of the property.	char	64
VALUE	The value for the property.	VARCHAR	2048

TABLE 143 OUI_VENDOR

Field	Definition	Format	Size
OUI*	Vendor OUI, 6-digit hexadecimal number which can have leading digits as zero.	char	6
VENDOR	Vendor name.	varchar	64

TABLE 144 OUI_GUESSED_DEVICE_MAP

Field	Definition	Format	Size
OUI*	Vendor OUI.	char	6
TYPE	Guessed device type for this vendor.	varchar	32

TABLE 145 FEATURE

Field	Definition	Format	Size
FEATURE_ID*	ID used to uniquely identify the feature.	int	6
NAME	Name of the feature.	varchar	256
DESCRIPTION	Description for the feature.	varchar	256

TABLE 146 FEATURE_EDITION_MAP

Field	Definition	Format	Size
FEATURE_ID*	ID used to uniquely identify the feature.	int	
EDITION_MASK	Used to associate a feature to the edition (Reserved for future).	int	

Port Fencing

TABLE 147 PORT_FENCING_POLICY

Field	Definition	Format	Size
ID*		int	
NAME	Name of the policy. The length of the field should be 62 because M-EOS switch supports only maximum 62 characters.	varchar	62
TYPE	0 = ISL Protocol 1 = Link 2 = Security	smallint	
THRESHOLD_LIMIT	Threshold Limits for M-EOS Switch.	int	
THRESHOLD_DURATION	Duration In minutes for M-EOS Switch.	int	
DEFAULT_POLICY	1 = the default port fencing policies. 0 = the non-default policies. The default port fencing policies are: For ISL - Default Protocol Error Policy For Link Violation type - Default Link Level Policy For Security - Default Security Policy	smallint	
B_THRESHOLD_LIMIT	Threshold Limits for Fabric OS Switch (Not Supported).	int	
B_THRESHOLD_DURATION	Duration in minutes for Fabric OS Switch (Not Supported).	int	

TABLE 148 PORT_FENCING_POLICY_MAP

Field	Definition	Format	Size
ID*		int	
POLICY_ID	Foreign key to ID column of PORT_FENCING_POLICY table.	int	
LEVEL	0 = All Fabric 1 = Fabric 2 = Core Switch Group 3 = Switch 4 = Port Type 5 = Port List	smallint	
SUB_LEVEL	1 = E_Port 2 = F_Port 3 = FL_Port, Fabric WWN, Switch WWN	char	23
NODE	WWN of Node which policy assigned.	char	23
INHERITANCE	Directly assigned or inherited from root level. 0 = Directly assigned 1 = Indirectly assigned	smallint	

Quartz

TABLE 149 QRTZ_JOB_DETAILS

Field	Definition	Format	Size
JOB_NAME*	Name of the job.	varchar	80
JOB_GROUP*	Name of the job group.	varchar	80
DESCRIPTION	Description of the job (optional).	varchar	120
JOB_CLASS_NAME	The instance of the job that will be executed.	varchar	128
IS_DURABLE	Whether the job should remain stored after it is orphaned.	bit	
IS_VOLATILE	Whether the job should not be persisted in the JobStore for re-use after program restarts.	bit	
IS_STATEFUL	Whether the job implements the interface StatefulJob.	bit	
REQUESTS_RECOVERY	Instructs the scheduler whether or not the job should be re-executed if a "recovery" or "fail-over" situation is encountered.	bit	
JOB_DATA	To persist the job-related and application-related informations.	image	

TABLE 150 QRTZ_TRIGGERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
JOB_NAME	Name of the job.	varchar	80
JOB_GROUP	Name of the job group.	varchar	80
IS_VOLATILE	Whether the trigger should be persisted in the JobStore for re-use after program restarts.	bit	
DESCRIPTION	A description for the trigger instance - may be useful for remembering/displaying the purpose of the trigger, though the description has no meaning to Quartz.	varchar	120
NEXT_FIRE_TIME	The next fire time in milliseconds.	numeric	13,0
PREV_FIRE_TIME	The previous fired time in milliseconds.	numeric	13,0
TRIGGER_STATE	The state of the trigger (viz. Error, wait,etc.)	varchar	16
TRIGGER_TYPE	The type of the trigger (Simple,cron).	varchar	8
START_TIME	The job start time.	numeric	13,0
END_TIME	The job end time (-1 means infinite).	numeric	13,0
CALENDAR_NAME		varchar	80
MISFIRE_INSTR	Instructs the scheduler to execute the misfired job.	smallint	
JOB_DATA	Persists the job-related info.	image	

TABLE 151 QRTZ_SIMPLE_TRIGGERS

Field	Definition	Format	size
TRIGGER_NAME*	Name of the trigger	varchar	80
TRIGGER_GROUP*	name of the trigger group	varchar	80
REPEAT_COUNT	number of times to repeat	numeric	13,0
REPEAT_INTERVAL	interval for first and second job	numeric	13,0
TIMES_TRIGGERED	Number of times the corresponding trigger fired	numeric	13,0

TABLE 152 QRTZ_FIRED_TRIGGERS

Field	Definition	Format	size
ENTRY_ID*	Fired instance ID.	varchar	95
TRIGGER_NAME	Name of the trigger.	varchar	80
TRIGGER_GROUP	Name of the trigger group.	varchar	80
IS_VOLATILE	Whether the job should not be persisted in the JobStore for re-use after the program restarts.	bit	
INSTANCE_NAME	Trigger instance name.	varchar	80
FIRED_TIME	The trigger fired time.	numeric	13,0
STATE	The fired trigger job state.	varchar	16
JOB_NAME	Name of the job.	varchar	80
JOB_GROUP	Name of the job group.	varchar	80
IS_STATEFUL	Whether the job implements the interface StatefulJob.	bit	
REQUESTS_RECOVERY	True or false.	bit	

TABLE 153 QRTZ_JOB_LISTENERS

Field	Definition	Format	Size
JOB_NAME*	Name of the job.	varchar	80
JOB_GROUP*	Name of the job group.	varchar	80
JOB_LISTENER*	Job listener action class instance.	varchar	80

TABLE 154 QRTZ_CRON_TRIGGERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
CRON_EXPRESSION	The CRON trigger Expression (ex:"0 0 12 * * ?" - meaning:Fire at 12pm (noon) every day).	varchar	80
TIME_ZONE_ID	Given "cron" expression resolved with respect to the TimeZone.	varchar	80

TABLE 155 QRTZ_JTRIGGER_LISTENERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
TRIGGER_LISTENER*	The listener action.	varchar	80

TABLE 156 QRTZ_BLOB_TRIGGERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
BLOB_DATA	The Scheduler info.	varchar	80

TABLE 157 QRTZ_SCHEDULER_STATE

Field	Definition	Format	Size
INSTANCE_NAME*	Instance of the scheduler.	varchar	80
LAST_CHECKIN_TIME	Last fired time in milliseconds.	numeric	13,0
CHECKIN_INTERVAL	Repeat interval.	numeric	13,0
RECOVERER	Misfire instruction.	varchar	80

TABLE 158 QRTZ_LOCKS

Field	Definition	Format	Size
LOCK_NAME*	Resource identification name assigned by user.	varchar	40

TABLE 159 QRTZ_CALENDARS

Field	Definition	Format	Size
CALENDAR_NAME*	Name of the Calendar.	varchar	80
CALENDAR	Calendar object.	image	

TABLE 160 QRTZ_PAUSED_TRIGGER_GRPS

Field	Definition	Format	Size
TRIGGER_GROUP*	Name of the trigger group.	varchar	80

Reports

TABLE 161 REPORT_TYPE

Field	Definition	Format	Size
ID*	Meta Data for available reports.	int	
NAME	Report name.	varchar	128
DESCRIPTION	Report type description.	varchar	256

TABLE 162 GENERATED_REPORT

Field	Definition	Format	Size
ID*		int	
NAME	Report name.	varchar	256
TYPE_ID	Report type.	int	
EFCM_USER	The Management application user who has generated this report.	varchar	128
REPORT_OBJECT	Report object BLOB.	image	
TIMESTAMP_	Timestamp when the report is generated.	timestamp	

Role Based Access Control

TABLE 163 USER_ROLE_MAP

Field	Definition	Format	Size
USER_NAME*	User name.	varchar	128
ROLE_ID*	Role ID, which is mapped for the user.	int	

TABLE 164 ROLE

Field	Definition	Format	Size
ID*		int	
NAME	Role name.	varchar	128
DESCRIPTION	Role description.	varchar	512

TABLE 165 ROLE_PRIVILEGE_MAP

Field	Definition	Format	Size
ROLE_ID*	User role ID.	int	
PRIVILEGE_ID*	Privilege ID.	int	
PERMISSION	Privilege permission: 1 = RO 2 = RW 0 = No privilege	smallint	

TABLE 166 PRIVILEGE

Field	Definition	Format	Size
ID*		int	
NAME	Privilege Name.	varchar	128

TABLE 167 PRIVILEGE_GROUP_MAP

Field	Definition	Format	Size
GROUP_ID*	Privilege group ID.	int	
PRIVILEGE_ID*	Privilege ID.	int	128

TABLE 168 PRIVILEGE_GROUP

Field	Definition	Format	Size
ID*		int	
NAME	Privilege group name.	varchar	128

TABLE 169 ROLE_PRIVILEGE_INFO

name	Source
ID	ROLE.ID
ROLE NAME	ROLE.NAME
ROLE DESCRIPTION	ROLE.DESCRIPTION
ID	PRIVILEGE.ID
NAME	PRIVILEGE.NAME
PERMISSION	ROLE_PRIVILEGE_MAP.PERMISSION

TABLE 170 USER_

Field	Definition	Format	Size
NAME*	User name.	varchar	128
DESCRIPTION	User description.	varchar	512
PASSWORD	User password.	varchar	512
EMAIL	User e-mail ID.	varchar	1024
NOTIFICATION_ENABLED	Flag for e-mail notification.	smallint	

TABLE 171 USER_RESOURCE_MAP

Field	Definition	Format	Size
USER_NAME*	User name.	varchar	128
RESOURCE_GROUP_ID*	Resource group name, which is mapped for the user.	int	

TABLE 172 RESOURCE_GROUP

Field	Definition	Format	Size
ID*		int	
NAME	Resource group name.	varchar	128
DESCRIPTION	Resource group description.	varchar	512

TABLE 173 RESOURCE_FABRIC_MAP

Field	Definition	Format	Size
RESOURCE_GROUP_ID*	Resource group ID.	int	
FABRIC_ID*	Fabric ID, which is in the resource group.	int	

TABLE 174 USER_ROLE_RESOURCE_INFO

name	Source
RESOURCE GROUP ID	RESOURCE_GROUP.ID RESOURCE_GROUP_ID
RESOURCE GROUP NAME	RESOURCE_GROUP.NAME RESOURCE_GROUP_NAME
ROLE ID	ROLE.ID ROLE_ID
ROLE NAME	ROLE.NAME ROLE_NAME
NAME	USER_.NAME USER_NAME

SNMP

TABLE 175 SNMP_CREDENTIALS

Field	Definition	Format	Size
ID*		int	
VIRTUAL SWITCH_ID	Virtual switch ID for which this instance of the SNMP credentials apply.	int	
RECIPIENT_ID	Recipient in the MESSAGE_RECIPIENT table.	int	
POR)_NUMBER	Port number of the SNMP agent on the switch for get and set requests.	smallint	
RETRY_COUNT	Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.	smallint	
TIMEOUT	Timeout value in seconds for a get/set request to the SNMP agent. Default value is 5.	smallint	
VERSION	SNMP agent version running on the switch, as in SNMPv1 or SNMPv3.	varchar	6
READ_COMMUNITY_ STRING	The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to a device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
WRITE_COMMUNITY_ STRING	The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to a device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
USER_NAME	A human readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
CONTEXT_NAME	Text ID associated with the user, used by the SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.	varchar	128
AUTH_PROTOCOL	An indication of whether messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. The supported values for this field are: usmNoAuthProtocol, usmHMACMD5AuthProtocol, and usmHMACSHAAuthProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
AUTH_PASSWORD	The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64

TABLE 175 SNMP_CREDENTIALS (Continued)

Field	Definition	Format	Size
PRIV_PROTOCOL	An indication of whether messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. The current values for this field are: usmNoPrivProtocol and usmDESPrivProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
PRIV_PASSWORD	The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64

TABLE 176 SNMP_PROFILE

Field	Definition	Format	Size
NAME*	A text string representing a set of SNMP agent profile. When created, one or more virtual switches could refer to this profile for its SNMP credentials unless a unique set of SNMP credentials has been defined in SNMP_CREDENTIAL.	varchar	256
PORT_NUMBER	Port number of the SNMP agent on the switch for get and set requests	smallint	
RETRY_COUNT	Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.	smallint	
TIMEOUT	Timeout value in seconds before for a get/set request to the SNMP agent. Default value is 5.	smallint	
VERSION	SNMP agent version running on the switch as in SNMPv1 and SNMPv3	varchar	6
READ_COMMUNITY_STRING	The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
WRITE_COMMUNITY_STRING	The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to a device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1	varchar	64
USER_NAME	A human-readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
CONTEXT_NAME	A text ID associated with the user, used by SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.	varchar	128

TABLE 176 SNMP_PROFILE (Continued)

Field	Definition	Format	Size
AUTH_PROTOCOL	An indication of whether or not messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. The supported values for this field are: usmNoAuthProtocol, usmHMACMD5AuthProtocol, and usmHMACSHAAuthProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
AUTH_PASSWORD	The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
PRIV_PROTOCOL	An indication of whether or not messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. The current values for this field are: usmNoPrivProtocol and usmDESPrivProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
PRIV_PASSWORD	The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64

TABLE 177 SNMP_V3_FORWARDING_CREDENTIAL

Field	Definition	Format	Size
ID*		int	
USER_NAME	USM user name.	varchar	64
CONTEXT_NAME	USM context name.	VARCHAR	128
AUTH_PROTOCOL	Authorization protocol.	VARCHA	16
AUTH_PASSWORD	Authorization password.	VARCHAR	64
PRIV_PROTOCOL	Privilege protocol.	VARCHAR	16
PRIV_PASSWORD	Privilege password.	VARCHAR	64

Stats

TABLE 178 FAVORITES

Field	Definition	Format	Size
ID*		int	
NAME	Name of the favorite.	varchar	64
USER_	The application user credentials.	varchar	128
TOP_N	The top number of ports(5,10,15,20).	varchar	40
SELECTION_FILTER	Types of ports (FC/FCIP/GE) and End-to-End Monitors.	varchar	40
FROM_TIME	The time interval in which the graph is shown. Time interval can be predefined or custom. If FROM_TIME is Custom, the user can choose the number of minutes/hours/days or specify the time interval.	varchar	40
CUSTOM_LAST_VALUE	The number of minutes/hours/days. It becomes null in two cases. 1. When the value of FROM_TIME is not Custom. 2. When FROM_TIME is Custom, and user chooses the time interval (CUSTOM_FROM and CUSTOM_TO)	int	
CUSTOM_TIME_UNIT	The unit type (Minutes, Hours, Days) of the CUSTOM_LAST_VALUE.	varchar	40
CUSTOM_FROM	The starting time.	timestamp	
CUSTOM_TO	The ending time.	timestamp	
GRANULARITY	The granularity.	varchar	40
THRESHOLD	The reference line.	int	
MAIN_MEASURE	The measure of FC/FCIP/GE.	varchar	40
ADDITIONAL_MEASURE	The additional measures.	int	

TABLE 179 USER_

Field	Definition	Format	Size
NAME*	User name.	varchar	128
DESCRIPTION	User description.	varchar	512
PASSWORD	User password.	varchar	512
EMAIL	User e-mail ID.	varchar	1024
NOTIFICATION_ENABLED	Flag for e-mail notification.	smallint	

TABLE 180 STATS_AGING

Field	Definition	Format	Size
ID*		int	
FIVE_MIN_VALUE	Configured maximum samples value for the five minute table.	int	
THIRTY_MIN_VALUE	Configured maximum samples value for the thirty minute table.	int	
TWO_HR_VALUE	Configured maximum samples value for the two hour table.	int	
ONE_DAY_VALUE	Configured maximum samples value for the one day table.	int	
MAX_SAMPLES_VALUE	The maximum number of samples value, i.e., 3456.	int	
INTERPOLATE	Whether interpolation is enabled or disabled.	smallint	

TABLE 181 MARCHING_ANTS

Field	Definition	Format	Size
ID*		int	
THRESHOLD1_VALUE	The marching ants low boundary threshold value (T1).	int	
THRESHOLD2_VALUE	The marching ants high boundary threshold value (T2).	int	

TABLE 182 DEFAULT_FAVORITES

Field	Definition	Format	Size
ID	Name of the favorite.	int	
NAME	The topnumber of ports (5,10,15,20).	varchar	64
TOP_N	Types of ports (FC/FCIP/GE) and End-to-End Monitors.	varchar	40
SELECTION_FILTER	The time interval in which the graph is shown.	varchar	40
FROM_TIME	Always null. The default favorite is not customized.	varchar	40
CUSTOM_LAST_VALUE	Always null. The default favorite is not customized.	int	
CUSTOM_TIME_UNIT	Always null. The default favorite is not customized.	varchar	40
CUSTOM_FROM	Always null. The default favorite is not customized.	timestamp	
CUSTOM_TO	The default five minutes granularity.	timestamp	
GRANULARITY	Always null.	varchar	40
THRESHOLD	The measure Tx MBps or Rx MBps based on DEFAULT_FAVORITES.NAME	int	
MAIN_MEASURE	The Additional measures based on the FAVORITE.MAIN_MEASURE	varchar	40
ADDITIONAL_MEASURE	The Additional measures based on the FAVORITE.MAIN_MEASURE	int	

Switch

TABLE 183 VIRTUAL-SWITCH

Field	Definition	Format	Size
ID*		int	
LOGICAL_ID	Logical ID of the switch.	smallint	
NAME	Switch name.	varchar	64
WWN	WWN of the switch.	char	23
VIRTUAL_FABRIC_ID	Virtual fabric ID. If VF enabled then will have the VFID; otherwise it will be -1.	smallint	
DOMAIN_ID	Domain ID of the switch.	smallint	
BASE_SWITCH	1 = this is a base switch; otherwise, 0.	smallint	
SWITCH_MODE	2 = switch is in AG mode; otherwise, 0.	smallint	
ROLE	Role of the switch.	varchar	32
FCS_ROLE	FCS role of the switch.	varchar	16
AD_CAPABLE	1 = switch is AD-capable.	smallint	
FABRIC_IDID_MODE	Fabric IDID mode.	smallint	
OPERATIONAL_STATUS	Operation status of switch.	varchar	128
MAX_ZONE_CONFIG_SIZE	Maximum size of zone configuration on the switch.	int	
CREATION_TIME	Time at which this record was created.	timestamp	
LAST_UPDATE_TIME	Time when this record was last updated.	timestamp	
USER_NAME	User name of the switch.	varchar	128
PASSWORD	Password.	varchar	128
MANAGEMENT_STATE	Various states as per manageability software like the Management application.	int	
STATE	State of the switch.	varchar	32
STATUS	Status of the switch.	varchar	32
STATUS_REASON	Reason for the status.	varchar	2048
USER_DEFINED_VALUE1		varchar	256
USER_DEFINED_VALUE2		varchar	256
USER_DEFINED_VALUE3		varchar	256
CORE_SWITCH_ID	Core switch DB ID.	int	
INTEROP_MODE	Mode in which this switch is operating.	smallint	
CRYPTO_CAPABLE	0 = the switch is not crypto-enabled; if capable it will have a non-zero value.	smallint	
FCR-CAPABLE	0 = the switch is not FCR-enabled; if capable it will have a non-zero value.	smallint	
FCIP_CAPABLE	0 = the switch is not FCIP-enabled; if capable it will have a non-zero value.	smallint	

TABLE 184 CORE_SWITCH

Field	Definition	Format	Size
ID*		int	
IP_ADDRESS	IP address of the switch.	varchar	128
WWN	Chassis WWN.	char	23
NAME	Switch name.	varchar	64
CONTACT	Any associated contact name, obtained through SNMP.	varchar	256
LOCATION	Physical location, obtained through SNMP.	varchar	256
DESCRIPTION	User assigned description, obtained through SNMP.	varchar	256
TYPE	SWBD type number as given by Fabric OS.	smallint	
MODEL	Model type of the switch: 0 = Unknown 1 = Not applicable 2 = Fabric OS switch 3 = M-EOS switch	smallint	
FIRMWARE_VERSION	Embedded (Fabric OS or M-EOS) software version.	varchar	128
VENDOR	Switch vendor.	varchar	256
MAX_VIRTUAL_SWITCHES	Maximum virtual switches allowed on this physical switch.	smallint	
NUM_VIRTUAL_SWITCHES	Actual number of virtual switches carved out of this physical switch. 0 means it is not operating in Virtual Fabric model.	smallint	
REACHABLE	Whether reachable by HTTP.	smallint	
UNREACHABLE_TIME	When the switch became unreachable from HTTP.	timestamp	
OPERATIONAL_STATUS	Operational status as reported by the embedded software.	varchar	128
CREATION_TIME	Time when this record was created by the Management application.	timestamp	
LAST_SCAN_TIME	Time when this record was last updated.	timestamp	
LAST_UPDATE_TIME	1 = the Management application server is registered with the switch to receive Syslog.	timestamp	
SYSLOG_REGISTERED	1 = Syslog is enabled for this switch.	smallint	
CALL_HOME_ENABLED	1 = call home is enabled for this switch.	smallint	
SNMP_REGISTERED	1 = the Management application server is registered with the switch to receive SNMP traps.	smallint	
USER_IP_ADDRESS	User-assigned IP address. This is used for M-EOS switches where Fabric OS seed switch fails to get the IP address of the M-EOS switch.	varchar	128

TABLE 184 CORE_SWITCH (Continued)

Field	Definition	Format	Size
NIC_PROFILE_ID	NIC profile of the Management application server host used by this switch to communicate in interactive configuration and other operations. It determines which Management application host IP used by this switch.	int	
MANAGING_SERVER_IP_ ADDRESS	IP address of the server which is currently managing this switch. Used for M-EOS switch only. It does not apply to Fabric OS switches.	varchar	128

TABLE 185 NIC_PROFILE

Field	Definition	Format	Size
ID*		int	
NAME	The name of the network interface in the format network interface name / host address.	varchar	255
IP_ADDRESS	The host address of the interface.	varchar	128

TABLE 186 SWITCH_INFO

name	Source
PHYSICAL SWITCH ID	CORE_SWITCH.ID
PHYSICAL SWITCH NAME	CORE_SWITCH.NAME
IP_ADDRESS	CORE_SWITCH.IP_ADDRESS
PHYSICAL SWITCH WWN	CORE_SWITCH.WWN
PHYSICAL OPERATIONAL STATUS	CORE_SWITCH.OPERATIONAL_STATUS
TYPE	CORE_SWITCH.TYPE
MAX_VIRTUAL_SWITCH	CORE_SWITCH.MAX_VIRTUAL_SWITCHES
NUM)VIRTUAL_SWITCHES	CORE_SWITCH.NUM_VIRTUAL_SWITCHES
FIRMWARE_VERSION	CORE_SWITCH.FIRMWARE_VERSION
VENDOR	CORE_SWITCH.VENDOR
REACHABLE	CORE_SWITCH.REACHABLE
UNREACHABLE_TIME	CORE_SWITCH.UNREACHABLE_TIME
CONTACT	CORE_SWITCH.CONTACT
LOCATION	CORE_SWITCH.LOCATION
DESCRIPTION	CORE_SWITCH.DESCRIPTION
MODEL	CORE_SWITCH.MODEL
SYSLOG_REGISTERED	CORE_SWITCH.SYSLOG_REGISTERED
SNMP_REGISTERED	CORE_SWITCH.SNMP_REGISTERED
CALL_HOME_ENABLED	CORE_SWITCH.CALL_HOME_ENABLED
USER_IP_ADDRESS	CORE_SWITCH.USER_IP_ADDRESS

TABLE 186 SWITCH_INFO

name	Source
NIC_PROFILE_ID	CORE_SWITCH.NIC_PROFILE_ID
MANAGING_SERVER_IP_ADDRESS	CORE_SWITCH.MANAGING_SERVER_IP_ADDRESS
ID	VIRTUAL_SWITCH.ID
NAME	VIRTUAL_SWITCH.NAME
OPERATIONAL_STATUS	VIRTUAL_SWITCH.OPERATIONAL_STATUS
SWITCH_MODE	VIRTUAL_SWITCH.SWITCH_MODE
AD_CAPABLE	VIRTUAL_SWITCH.AD_CAPABLE
WWN	VIRTUAL_SWITCH.WWN
ROLE	VIRTUAL_SWITCH.ROLE
FCS_ROLE	VIRTUAL_SWITCH.FCS_ROLE
DOMAIN_ID	VIRTUAL_SWITCH.DOMAIN_ID
VIRTUAL_FABRIC_ID	VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID
BASE_SWIITCH	VIRTUAL_SWITCH.BASE_SWITCH
MAX_ZONE_CONFIG_SIZE	VIRTUAL_SWITCH.MAX_ZONE_CONFIG_SIZE
CREATION_TIME	VIRTUAL_SWITCH.CREATION_TIME
LAST_UPDATE_TIME	VIRTUAL_SWITCH.LAST_UPDATE_TIME
USER_NAME	VIRTUAL_SWITCH.USER_NAME
PASSWORD	VIRTUAL_SWITCH.PASSWORD
MANAGEMENT_STATE	VIRTUAL_SWITCH.MANAGEMENT_STATE
STATE	VIRTUAL_SWITCH.STATE
STATUS	VIRTUAL_SWITCH.STATUS
STATUS_REASON	VIRTUAL_SWITCH.STATUS_REASON
FABRIC_IDID_MODE	VIRTUAL_SWITCH.FABRIC_IDID_MODE
LOGICAL_ID	VIRTUAL_SWITCH.LOGICAL_ID
USER_DEFINED_VALUE_1	VIRTUAL_SWITCH.USER_DEFINED_VALUE_1
USER_DEFINED_VALUE_2	VIRTUAL_SWITCH.USER_DEFINED_VALUE_2
USER_DEFINED_VALUE_3	VIRTUAL_SWITCH.USER_DEFINED_VALUE_3
INTEROP_MODE	VIRTUAL_SWITCH.INTEROP_MODE
CRYPTO_CAPABLE	VIRTUAL_SWITCH.CRYPTO_CAPABLE
FCR_CAPABLE	VIRTUAL_SWITCH.FCR_CAPABLE
FCIP_CAPABLE	VIRTUAL_SWITCH.FCIP_CAPABLE
FABRIC_ID	FABRIC_MEMBER.FABRIC_ID
TRUSTED	FABRIC_MEMBER.TRUSTED
MISSING	FABRIC_MEMBER.MISSING
MISSING_TIME	FABRIC_MEMBER.MISSING_TIME

TABLE 187 SWITCH_MODEL

Field	Definition	Format	Size
ID*		int	
SWBD_TYPE	Switch type number, universally used by all the Management application module implementation.	smallint	
SUBTYPE	Switch subtype. At present no subtypes for existing model records are defined.	smallint	
DESCRIPTION	Model description, such as FC link speed, port count and whether multi-card (director) class switch or other type of switch.	varchar	32
MODEL	Switch model string.	varchar	32
REMARK	Remarks, such as an internal project name.	varchar	64

TABLE 188 PURGED_SWITCH

Field	Definition	Format	Size
WWN*	WWN of the switch.	char	23
NAME	Name of the switch.	varchar	64
VIRTUAL_FABRIC_ID	Virtual fabric ID.	smallint	
USER_NAME	Switch user name.	varchar	64
PASSWORD	Switch password.	varchar	128
IP_ADDRESS	IP address.	varchar	128
PORT_NUMBER	SNMP port number.	smallint	
RETRY_COUNT	Retry count.	smallint	
TIMEOUT	SNMP time out value.	smallint	
VERSION	SNMP version.	varchar	6
READ_COMMUNITY_STRING	Read community string.	varchar	64
WRITE_COMMUNITY_STRING	Write community string.	varchar	64
SNMP_USER_NAME	SNMP user name.	varchar	128
CONTEXT_NAME	SNMP context name.	varchar	128
AUTH_PROTOCOL	SNMP auth protocol.	varchar	16
AUTH_PASSWORD	snmp auth password	varchar	64
PRIV_PROTOCOL	snmp priv protocol	varchar	16
PRIV_PASSWORD	snmp priv password	varchar	64

Switch details

TABLE 189 CORE_SWITCH_DETAILS

Field	Definition	Format	Size
CORE_SWITCH_ID*	DB ID.	int	
ETHERNET_MASK	Subnet mask.	char	64
FC_MASK	Subnet mask for FC IP.	char	64
FC_IP	Fibre Channel IP address.	char	64
FC_CERTIFICATE		smallint	
SW_LICENSE_ID		char	23
SUPPLIER_SERIAL_ NUMBER	Serial number of the chassis.	varchar	32
PART_NUMBER	The part number assigned by the organization responsible for producing or manufacturing the PhysicalElement.	varchar	32
CHECK_BEACON	1 = beacon is turned on; otherwise, 0.	smallint	
TIMEZONE	Time zone configured on the switch.	varchar	32
FMS_MODE	1 = FICON Management Server mode is enabled on the switch.	smallint	
MAX_PORT	Number of maximum ports physically allowed on the switch.	smallint	
CHASSIS_SERVICE_TAG		varchar	32
BAY_ID		varchar	32
TYPE_NUMBER		varchar	32
MODEL_NUMBER	Switch model number / string.	varchar	32
MANUFACTURER	The name of the organization responsible for producing the chassis. This might be different from the vendor if the product is shipped by an OEM with a private label.	varchar	32
PLANT_OF_MANUFACTURE R	Plant where the switch is manufactured.	varchar	32
SEQUENCE_NUMBER	Serial number of the switch.	varchar	32
TAG	An arbitrary string that uniquely identifies the chassis and serves as its physical key. The Tag property contains the WWN of the license switch (LicenseWWN).	varchar	32
DYNAMIC_LOAD_SHARING		smallint	
PORT_BASED_ROUTING		smallint	
IN_ORDER_DELIVERY		smallint	
ACT_CP_PRI_FW_VERSION	Active CP primary firmware version.	varchar	128
ACT_CP_SEC_FW_VERSION	Active CP secondary firmware version.	varchar	128

TABLE 189 CORE_SWITCH_DETAILS (Continued)

Field	Definition	Format	Size
STBY_CP_PRI_FW_VERSION	Standby CP primary firmware version.	varchar	128
STBY_CP_SEC_FW_VERSION	Standby CP secondary firmware version.	varchar	128
TYPE	SWBD number as assigned by embedded SW depending upon the switch type / platform.	smallint	
EGM_CAPABLE	1 = the switch is EGM-capable.	smallint	
SUB_TYPE	SWBD sub type number.	varchar	32
INSISTENT_DID_MODE	1 = insistent domain ID mode is enabled on the switch.	smallint	
PARTITION		smallint	

TABLE 190 CORE_SWITCH

Field	Definition	Format	Size
ID*		int	
IP_ADDRESS	IP address of the switch.	varchar	128
WWN	Chassis WWN.	char	23
NAME	Switch name.	varchar	64
CONTACT	Any associated contact name, obtained through SNMP.	varchar	256
LOCATION	Physical location, obtained through SNMP.	varchar	256
DESCRIPTION	User assigned description, obtained through SNMP.	varchar	256
TYPE	SWBD type number as given by Fabric OS.	smallint	
MODEL	Model type of the switch: 0 = Unknown 1 = Not applicable 2 = Fabric OS switch 3 = M-EOS switch	smallint	
FIRMWARE_VERSION	Embedded (Fabric OS or M-EOS) software version.	varchar	128
VENDOR	Switch vendor.	varchar	256
MAX_VIRTUAL_SWITCHES	Maximum virtual switches allowed on this physical switch.	smallint	
NUM_VIRTUAL_SWITCHES	Actual number of virtual switches carved out of this physical switch. 0 means it is not operating in Virtual Fabric model.	smallint	
REACHABLE	Whether reachable by HTTP.	smallint	
UNREACHABLE_TIME	When the switch became unreachable from HTTP.	timestamp	
OPERATIONAL_STATUS	Operational status as reported by the embedded software.	varchar	128
CREATION_TIME	Time when this record is created by the Management application.	timestamp	

TABLE 190 CORE_SWITCH (Continued)

Field	Definition	Format	Size
LAST_SCAN_TIME		timestampty	
LAST_UPDATE_TIME	Time when this record was last updated.	timestamp	
SYSLOG_REGISTERED	1 if the Management application server is registered with the switch to receive Syslog.	smallint	
CALL_HOME_ENABLED	1 if "call home" is enabled for this switch.	smallint	
SNMP_REGISTERED	1 if the Management application server is registered with the switch to receive SNMP traps.	smallint	
USER_IP_ADDRESS	User assigned IP address. This is used for M-EOS switches where Fabric OS seed switch fails to get the IP address of the M-EOS switch.	varchar	128
NIC_PROFILE_ID	NIC profile of the Management application server host used by this switch to communicate in interactive configuration and other operations. It determines which Management application host IP used by this switch.	int	
MANAGING_SERVER_IP_ ADDRESS	IP address of the server which is currently managing this switch. Used for M-EOS switch only. It does not apply for Fabric OS switches.	varchar	128

TABLE 191 SWITCH_DETAILS_INFO

Name	Source
PHYSICAL SWITCH ID	CORE_SWITCH.ID
PHYSICAL SWITCH NAME	CORE_SWITCH.NAME
IP_ADDRESS	CORE_SWITCH.IP_ADDRESS
PHYSICAL SWITCH WWN	CORE_SWITCH.WWN
PHYSICAL OPERATIONAL STATUS	CORE_SWITCH.OPERATIONAL_STATUS
TYPE	CORE_SWITCH.TYPE
MAX_VIRTUAL_SWITCHES	CORE_SWITCH.MAX_VIRTUAL_SWITCHES
FIRMWARE_VERSION	CORE_SWITCH.FIRMWARE_VERSION
VENDOR	CORE_SWITCH.VENDOR
REACHABLE	CORE_SWITCH.REACHABLE
UNREACHABLE_TIME	CORE_SWITCH.UNREACHABLE_TIME
CONTACT	CORE_SWITCH.CONTACT
LOCATION	CORE_SWITCH.LOCATION
DESCRIPTION	CORE_SWITCH.DESCRIPTION
MODEL	CORE_SWITCH.MODEL
SYSLOG_REGISTERED	CORE_SWITCH.SYSLOG_REGISTERED
SNMP_REGISTERED	CORE_SWITCH.SNMP_REGISTERED
USER_IP_ADDRESS	CORE_SWITCH.USER_IP_ADDRESS

TABLE 191 SWITCH_DETAILS_INFO

Name	Source
MANAGING_SERVER_IP_ADDRESS	CORE_SWITCH.MANAGING_SERVER_IP_ADDRESS
ID	VIRTUAL_SWITCH.ID
NAME	VIRTUAL_SWITCH.NAME
OPERATIONAL_STATUS	VIRTUAL_SWITCH.OPERATIONAL_STATUS
SWITCH_MODE	VIRTUAL_SWITCH.SWITCH_MODE
AD_CAPABLE	VIRTUAL_SWITCH.AD_CAPABLE
WWN	VIRTUAL_SWITCH.WWN
ROLE	VIRTUAL_SWITCH.ROLE
FCS_ROLE	VIRTUAL_SWITCH.FCS_ROLE
DOMAIN_ID	VIRTUAL_SWITCH.DOMAIN_ID
VIRTUAL_FABRIC_ID	VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID
BASE_SWITCH	VIRTUAL_SWITCH.BASE_SWITCH
MAX_ZONE_CONFIG_SIZE	VIRTUAL_SWITCH.MAX_ZONE_CONFIG_SIZE
CREATION_TIME	VIRTUAL_SWITCH.CREATION_TIME
LAST_UPDATE_TIME	VIRTUAL_SWITCH.LAST_UPDATE_TIME
USER_NAME	VIRTUAL_SWITCH.USER_NAME
PASSWORD	VIRTUAL_SWITCH.PASSWORD
MANAGEMENT_STATE	VIRTUAL_SWITCH.MANAGEMENT_STATE
STATE	VIRTUAL_SWITCH.STATE
STATUS	VIRTUAL_SWITCH.STATUS
STATUS_REASON	VIRTUAL_SWITCH.STATUS_REASON
FABRIC_IDID_MODE	VIRTUAL_SWITCH.FABRIC_IDID_MODE
LOGICAL_ID	VIRTUAL_SWITCH.LOGICAL_ID
USER_DEFINED_VALUE_1	VIRTUAL_SWITCH.USER_DEFINED_VALUE_1
USER_DEFINED_VALUE_2	VIRTUAL_SWITCH.USER_DEFINED_VALUE_2
USER_DEFINED_VALUE_3	VIRTUAL_SWITCH.USER_DEFINED_VALUE_3
FABRIC_ID	FABRIC_MEMBER.FABRIC_ID
TRUSTED	FABRIC_MEMBER.TRUSTED
MISSING	FABRIC_MEMBER.MISSING
MISSING_TIME	FABRIC_MEMBER.MISSING_TIME
ETHERNET_MASK	CORE_SWITCH_DETAILS.ETHERNET_MASK
FC_MASK	CORE_SWITCH_DETAILS.FC_MASK
FC_IP	CORE_SWITCH_DETAILS.FC_IP
FC_CERTIFICATE	CORE_SWITCH_DETAILS.FC_CERTIFICATE
SW_LICENSE_ID	CORE_SWITCH_DETAILS.SW_LICENSE_ID
SUPPLIER_SERIAL_NUMBER	CORE_SWITCH_DETAILS.SUPPLIER_SERIAL_NUMBER

TABLE 191 SWITCH_DETAILS_INFO

Name	Source
PART_NUMBER	CORE_SWITCH_DETAILS.PART_NUMBER
CHECK_BEACON	CORE_SWITCH_DETAILS.CHECK_BEACON
TIMEZONE	CORE_SWITCH_DETAILS.TIMEZONE
FMS_MODE	CORE_SWITCH_DETAILS.FMS_MODE
MAX_PORT	CORE_SWITCH_DETAILS.MAX_PORT
CHASSIS_SERVICE_TAG	CORE_SWITCH_DETAILS.CHASSIS_SERVICE_TAG
BAY_ID	CORE_SWITCH_DETAILS.BAY_ID
TYPE_NUMBER	CORE_SWITCH_DETAILS.TYPE_NUMBER
MODEL_NUMBER	CORE_SWITCH_DETAILS.MODEL_NUMBER
MANUFACTURER	CORE_SWITCH_DETAILS.MANUFACTURER
PLANT_OF_MANUFACTURER	CORE_SWITCH_DETAILS.PLANT_OF_MANUFACTURER
SEQUENCE_NUMBER	CORE_SWITCH_DETAILS.SEQUENCE_NUMBER
TAG	CORE_SWITCH_DETAILS.TAG
DYNAMIC_LOAD_SHARING	CORE_SWITCH_DETAILS.DYNAMIC_LOAD_SHARING
PORT_BASED_ROUTING	CORE_SWITCH_DETAILS.PORT_BASED_ROUTING
IN_ORDER_DELIVERY	CORE_SWITCH_DETAILS.IN_ORDER_DELIVERY
ACT_CP_PRI_FW_VERSION	CORE_SWITCH_DETAILS.ACT_CP_PRI_FW_VERSION
ACT_CP_SEC_FW_VERSION	CORE_SWITCH_DETAILS.ACT_CP_SEC_FW_VERSION
STBY_CP_PRI_FW_VERSION	CORE_SWITCH_DETAILS.STBY_CP_PRI_FW_VERSION
STBY_CP_SEC_FW_VERSION	CORE_SWITCH_DETAILS.STBY_CP_SEC_FW_VERSION
DETAILS TYPE	CORE_SWITCH_DETAILS.TYPE as DETAILS_TYPE
EGM_CAPABLE	CORE_SWITCH_DETAILS.EGM_CAPABLE
SUB_TYPE	CORE_SWITCH_DETAILS.SUB_TYPE
INSISTENT_DID_MODE	CORE_SWITCH_DETAILS.INSISTENT_DID_MODE
PARTITION	CORE_SWITCH_DETAILS.PARTITION

Switch port

TABLE 192 GIGE_PORT

Field	Definition	Format	Size
ID*		int	
SWITCH_PORT_ID	ID for the GigE Port in SWITCH_PORT.	int	
PORT_NUMBER	GigE Port Number(0 for ge0 and 1 for ge1).	int	
SLOT_NUMBER	Slot number on which the GigE Port is present.	int	
ENABLED	Enabled or disabled.	smallint	
SPEED	Port speed details.	int	
MAX_SPEED	Port maximum speed supported.	int	
MAC_ADDRESS	MAC Address of that port.	varchar	64
PORT_NAME	GigE Port Name.	varchar	64
OPERATIONAL_STATUS	LED status.	int	
LED_STATE	LED status.	smallint	
SPEED_LED_STATE	GigE Port type details.	smallint	
PORT_TYPE	Port type for the GigE Port.	varchar	64
PERSISTENTLY_DISABLED	Whether the GigE Port is persistently disabled.	smallint	
INTERFACE_TYPE		smallint	
CHECKSUM		varchar	16
FCIP_CAPABLE	1 = FCIP capable; otherwise, 0.	smallint	
ISCSI_CAPABLE	1 = ISCSI capable; otherwise, 0.	smallint	
INBAND_MANAGEMENT_STATUS	1 = Inband Management status is enabled; otherwise, 0.	smallint	

TABLE 193 SWITCH_PORT

Field	Definition	Format	Size
ID*		int	
VIRTUAL_SWITCH_ID	DB ID of virtual_switch to which this port belongs.	int	
WWN	WWN of the port.	char	23
NAME	User friendly name of the port.	char	32
SLOT_NUMBER	Slot number.	int	
PORT_NUMBER	The logical port number of the user port. There is no assumption of any relation to the physical location of a port within a chassis.	smallint	
USER_PORT_NUMBER	User port number. Unique port number in a chassis.	smallint	
PORT_ID	Port ID of this port.	varchar	8
PORT_INDEX	Number used for identifying port in zoning.	smallint	
AREA_ID	Area number the port is assigned to.	smallint	

TABLE 193 SWITCH_PORT (Continued)

Field	Definition	Format	Size
MAC_ADDRESS	MAC address of this port.	varchar	64
PORT_MOD		varchar	64
TYPE	Port type. The specific mode currently enabled for the port.	varchar	16
FULL_TYPE	Port type.	varchar	128
STATUS	The current status of the switch port.	varchar	64
HEALTH		varchar	16
STATUS_MESSAGE	Status message if any.	varchar	255
PHYSICAL_PORT	1 = it is a physical port 0 = it is a virtual port	smallint	
LOCKED_PORT_TYPE	Locked port type.	varchar	16
CATEGORY		smallint	
PROTOCOL		varchar	16
SPEED	Actual speed at which the port is currently operating.	varchar	64
SPEEDS_SUPPORTED	Supported speed values.	varchar	32
MAX_PORT_SPEED	The maximum speed the port is capable of supporting, in bits per second.	int	
DESIRED_CREDITS	How many BB credits are desired for the port.	int	
BUFFER_ALLOCATED	How many BB credits are allocated for the port.	int	
ESTIMATED_DISTANCE	The estimated physical distance of the connection between ports.	int	
ACTUAL_DISTANCE	The physical distance of the connection on the port in relation to the other port.	int	
LONG_DISTANCE_SETTING	Whether long distance enabled.	int	
DEGRADED_PORT	Whether a port is degraded or not.	varchar	16
REMOTE_NODE_WWN	Node WWN of the attached port.	varchar	255
REMOTE_PORT_WWN	WWN of the attached port.	varchar	255
LICENSED	1 = the port is licensed; otherwise, 0.	smallint	
SWAPPED	1 = port is swapped; otherwise, 0.	smallint	
TRUNKED	1 = port is trunked; otherwise, 0.	smallint	
TRUNK_MASTER	1 = the port is trunk master; otherwise, 0.	smallint	
PERSISTENT_DISABLE	1 = port is persistently disabled.	smallint	
FICON_SUPPORTED	1 = FICON is supported; otherwise, 0.	smallint	
BLOCKED	1 = port is blocked; otherwise, 0.	smallint	
PROHIBIT_PORT_NUMBERS		varchar	255
PROHIBIT_PORT_COUNT		smallint	
NPIV	Whether NPIV mode is enabled.	smallint	

TABLE 193 SWITCH_PORT (Continued)

Field	Definition	Format	Size
NPIV_CAPABLE	Instance NPIV mode capability: 1 = indicates port has NPIV capability 2 = NPIV license is enabled	smallint	
NPIV_ENABLED	Whether NPIV mode is enabled.	smallint	
FC_FAST_WRITE_ENABLED	1 = FC fast write is enabled.	smallint	
ISL_RRDY_ENABLED		smallint	
RATE_LIMIT_CAPABLE		smallint	
RATE_LIMITED		smallint	
QOS_CAPABLE		smallint	
TUNNEL_CONFIGURED		smallint	
FCIP_TUNNEL_UP		smallint	
FCR_FABRIC_ID		smallint	
FCR_INTEROP_MODE		smallint	
CALCULATED_STATUS		varchar	64
USER_DEFINED_VALUE1		varchar	256
USER_DEFINED_VALUE2		varchar	256
USER_DEFINED_VALUE3		varchar	256
KIND		varchar	32
STATE		varchar	64

TABLE 194 GIGE_PORT_INFO

name	Source
ID	GIGE_PORT.ID
SWITCH_PORT_ID	GIGE_PORT.SWITCH_PORT_ID
PORT_NUMBER	GIGE_PORT.PORT_NUMBER
SLOT_NUMBER	GIGE_PORT.SLOT_NUMBER
ENABLED	GIGE_PORT.ENABLED
SPEED	GIGE_PORT.SPEED
MAX_SPEED	GIGE_PORT.MAX_SPEED
MAC_ADDRESS	GIGE_PORT.MAC_ADDRESS
PORT_NAME	GIGE_PORT.PORT_NAME
OPERATIONAL_STATUS	GIGE_PORT.OPERATIONAL_STATUS
LED_STATE	GIGE_PORT.LED_STATE
SPEED_LED_STATE	GIGE_PORT.SPEED_LED_STATE
PORT_TYPE	GIGE_PORT.PORT_TYPE
PERSISTENTLY_DISABLED	GIGE_PORT.PERSISTENTLY_DISABLED

TABLE 194 GIGE_PORT_INFO (Continued)

name	Source
INTERFACE_TYPE	GIGE_PORT.INTERFACE_TYPE
CHECKSUM	GIGE_PORT.CHECKSUM
FCIP_CAPABLE	GIGE_PORT.FCIP_CAPABLE
ISCSI_CAPABLE	GIGE_PORT.ISCSI_CAPABLE
INBAND_MANAGEMENT_STATUS	GIGE_PORT.INBAND_MANAGEMENT_STATUS
VIRTUAL SWITCHID	SWITCH_PORT.VIRTUAL_SWITCH_ID
USER PORT NUMBER	SWITCH_PORT.USER_PORT_NUMBER

TABLE 195 N2F_PORT_MAP

Field	Definition	Format	Size
ID*		INT	
VIRTUAL_SWITCH_ID	Virtual switch ID of AG for N to F_port mapping, foreign key to VIRTUAL_SWITCH table.	INT	
N_PORT	Port number of port type N_Port which is being mapped, One N_Port can be mapped to multiple F_ports.	SMALLINT	
F_PORT	Port number of port type F_Port which is being mapped.	SMALLINT	

TABLE 196 N2F_PORT_MAP_INFO

Name	Source
VIRTUAL SWITCHID	N2F_PORT_MAP.VIRTUAL_SWITCH_ID
N PORT	N2F_PORT_MAP.N_PORT
F PORT	N2F_PORT_MAP.F_PORT
EDGE SWITCH PORT WWN	AG_N_PORT.REMOTE_PORT_WWN
AG F PORT WWN	AG_F_PORT.WWN
REMOTE NODE WWN	AG_F_PORT.REMOTE_NODE_WWN
DEVICE PORT WWN	AG_F_PORT.REMOTE_PORT_WWN

TABLE 197 FPORT_TRUNK_GROUP

Field	Definition	Format	Size
ID*		INT	
VIRTUAL_SWITCH_ID	Virtual switch ID where this F_Port Trunk Group is defined.	INT	
MASTER_USER_PORT	User port number for the master port of this trunk.	SMALLINT	
WWN	WWN of the trunk group.	CHAR	23
TRUNK_AREA	User-assigned area number used to group together F_ports of the trunk.	SMALLINT	

TABLE 198 FPORT_TRUNK_MEMBER

Field	Definition	Format	Size
GROUP_ID*	Foreign key to the PORT_TRUNK_GROUP table.	INT	
PORT_NUMBER*	Member user port number.	SMALLINT	
WWN	Member port WWN.	CHAR	23

TABLE 199 VIRTUAL_SWITCH

Field	Definition	Format	Size
ID*		int	
LOGICAL_ID	Logical ID of the switch.	smallint	
NAME	Switch name.	varchar	64
WWN	WWN of the switch.	char	23
VIRTUAL_FABRIC_ID	Virtual fabric ID. If VF enabled then will have the VFID; otherwise, it will be -1	smallint	
DOMAIN_ID	Domain ID of the switch.	smallint	
BASE_SWITCH	1 = this is a base switch; otherwise, 0.	smallint	
SWITCH_MODE	2 = switch is in AG mode; otherwise, 0.	smallint	
ROLE	Role of the switch.	varchar	32
FCS_ROLE	FCS role of the switch.	varchar	16
AD_CAPABLE	1 = switch is AD-capable.	smallint	
FABRIC_IDID_MODE	Fabric IDID mode.	smallint	
OPERATIONAL_STATUS	Operation status of switch.	varchar	128
MAX_ZONE_CONFIG_SIZE	Maximum size of zone configuration on the switch.	int	
CREATION_TIME	Time at which this record was created.	timestamp	
LAST_UPDATE_TIME	Time when this record was last updated.	timestamp	
USER_NAME	User name of the switch.	varchar	128
PASSWORD	Password.	varchar	128
MANAGEMENT_STATE	Various states as per manageability software like the Management application.	int	
STATE	State of the switch.	varchar	32
STATUS	Status of the switch.	varchar	32
STATUS_REASON	Reason for the status.	varchar	2048
USER_DEFINED_VALUE_1		varchar	256
USER_DEFINED_VALUE_2		varchar	256
USER_DEFINED_VALUE_3		varchar	256
CORE_SWITCH_ID	Core switch DB ID.	int	
INTEROP_MODE	Mode in which this switch is operating.	smallint	

TABLE 199 VIRTUAL_SWITCH (Continued)

Field	Definition	Format	Size
CRYPTO_CAPABLE	0 = the switch is not crypto-enabled; if capable it will have non-zero value	smallint	
FCR_CAPABLE	0 = the switch is not FCR-enabled; if capable it will have non-zero value	smallint	
FCIP_CAPABLE	0 if the switch is not FCIP-enabled; if capable it will have non-zero value	smallint	

Switch SNMP info

TABLE 200 VIRTUAL_SWITCH

Name	Source
PHYSICAL SWITCH ID	PHYSICAL_SWITCH_ID
PHYSICAL SWITCH NAME	PHYSICAL_SWITCH_NAME
IP ADDRESS	IP_ADDRESS
PHYSICAL SWITCH WWN	PHYSICAL_SWITCH_WWN
PHYSICAL OPERATIONAL STATUS	PHYSICAL_OPERATIONAL_STATUS
TYPE	TYPE
MAX VIRTUAL SWITCHES	MAX_VIRTUAL_SWITCHES
FIRMWARE VERSION	FIRMWARE_VERSION
VENDOR	VENDOR
REACHABLE	REACHABLE
UNREACHABLE TIME	UNREACHABLE_TIME
CONTACT	CONTACT
LOCATION	LOCATION
DESCRIPTION	DESCRIPTION
MODEL	MODEL
ID	SWITCH_INFO.ID
NAME	SWITCH_INFO.NAME
OPERATIONAL STATUS	OPERATIONAL_STATUS
SWITCH MAODE	SWITCH_MODE
AD CAPABLE	AD_CAPABLE
WWN	WWN
ROLE	ROLE
FCS ROLE	FCS_ROLE
DOMAIN ID	DOMAIN_ID
VIRTUAL FABRIC ID	VIRTUAL_FABRIC_ID

TABLE 200 VIRTUAL_SWITCH

Name	Source
BASE SWITCH	BASE_SWITCH
MAX ZONE CONFIG SIZE	MAX_ZONE_CONFIG_SIZE
CREATION TIME	CREATION_TIME
LAST UPDATE TIME	LAST_UPDATE_TIME
USER NAME	SWITCH_INFO.USER_NAME
PASSWORD	PASSWORD
MANAGEMENT STATE	MANAGEMENT_STATE
STATE	STATE
STATUS	STATUS
STATUS REASON	STATUS_REASON
USER DEFINED VALUE1	USER_DEFINED_VALUE_1
USER DEFINED VALUE2	USER_DEFINED_VALUE_2
USER DEFINED VALUE3	USER_DEFINED_VALUE_3
FABRIC ID	FABRIC_ID
TRUSTED	TRUSTED
MISSING	MISSING
MISSING TIME	MISSING_TIME
SNMP PORT NUMBER	SNMP_CREDENTIALS.PORT_NUMBER
SNMP RETRY COUNT	SNMP_CREDENTIALS.RETRY_COUNT
SNMP TIMEOUT	SNMP_CREDENTIALS.TIMEOUT
SNMP VERSION	SNMP_CREDENTIALS.VERSION
SNMP READ COMUMUNITY STRING	SNMP_CREDENTIALS.READ_COMMUNITY_STRING
SNMP WRITE COMMUNITY STRING	SNMP_CREDENTIALS.WRITE_COMMUNITY_STRING
SNMP USER NAME	SNMP_CREDENTIALS.USER_NAME
SNMP CONTEXT NAME	SNMP_CREDENTIALS.CONTEXT_NAME
SNMP AUTH PROTOCOL	SNMP_CREDENTIALS.AUTH_PROTOCOL
SNMP AUTH PASSWORD	SNMP_CREDENTIALS.AUTH_PASSWORD
SNMP PRIV PROTOCOL	SNMP_CREDENTIALS.PRIV_PROTOCOL
SNMP PRIV PASSWORD	SNMP_CREDENTIALS.PRIV_PASSWORD

Threshold

TABLE 201 SWITCH_THRESHOLD-SETTING

Field	Definition	Format	Size
SWITCH_ID*	References the ID in CORE_SWITCH table.	int	
POLICY_ID*	References the ID in THRESHOLD_POLICY table.	int	
STATUS	The status of applied to the switch.	smallint	
OVERRIDDEN	Policy is overridden or not overridden.	smallint	
DESCRIPTION	Description about the status of policy applied to the switch.	varchar	100

TABLE 202 THRESHOLD_POLICY

Field	Definition	Format	Size
ID*		int	
NAME	Name of the policy.	varchar	24
TYPE	Type of the policy.	varchar	20
DESCRIPTION	Description about the policy.	varchar	100

TABLE 203 FABRIC_THRESHOLD_SETTING

Field	Definition	Format	Size
FABRIC_ID*	References the ID in FABRIC table	int	
POLICY_ID*	References the ID in THRESHOLD_POLICY table	int	24

TABLE 204 VIRTUAL_SWITCH

Field	Definition	Format	Size
ID*		INT	

TABLE 205 PM_MEASURE

Field	Definition	Format	Size
ID*		int	
DESCRIPTION	The description of the measure.	varchar	64
NAME	Name of the measure.	varchar	32

TABLE 206 THRESHOLD_MEASURE

Field	Definition	Format	Size
MEASURE_ID*	References the ID In PM_MEASURE table, where all measures are defined.	int	
HIGH_BOUNDARY	Configured high boundary threshold value for measure ID.	int	

TABLE 206 THRESHOLD_MEASURE (Continued)

Field	Definition	Format	Size
LOW_BOUNDARY	Configured low boundary threshold value for measure ID.	int	
BUFFER_SIZE	Configured buffer size for measure ID.	int	
POLICY_ID*	References the ID in THRESHOLD_POLICY table.	int	

User Interface

TABLE 207 AVAILABLE_FLYOVER_PROPERTY

Field	Definition	Format	Size
ID*		int	
NAME	Name of the available property to be included in the flyover display.	varchar	40
TYPE	The flyover property type: 0 = Product property 1 = Connection property	smallint	
DEFAULT_SELECTION	AVAILABLE_FLYOVER_PROPERTY DEFAULT_SELECTION 1 = default selected product/connection property 0 = not included in the default list.	smallint	

TABLE 208 SELECTED_FLYOVER_PROPERTY

Field	Definition	Format	Size
PROPERTY_ID*	Refers to Flyover_Property ID from AVAILABLE_FLYOVER_PROPERTY table.	int	
USER_NAME*	The name of the user who selected the property to be shown on flyover.	varchar	128

TABLE 209 TOOL_APP

Field	Definition	Format	Size
TOOL_MENU_TEXT*	Text to be displayed for the Tool Menu.	varchar	256
TOOL_ID	A Tool in the TOOL_PATH table where the tools are defined.	int	
PARAMETERS	Default path for launching the tool.	varchar	256
KEY_STROKE	Short cut key stroke to the application.	varchar	30

TABLE 210 TOOL_PATH

Field	Definition	Format	Size
ID*		int	
TOOL_NAME	Name of the tool.	varchar	256

TABLE 210 TOOL_PATH (Continued)

Field	Definition	Format	Size
PATH	Path of the tool where installed or available.	varchar	1057
WORKING_FOLDER	Working folder for that application.	varchar	512

TABLE 211 PRODUCT_APP

Field	Definition	Format	Size
ID*		int	
MENU_TEXT	Name of the product menu.	varchar	256
PROP1_KEY	First condition name to be satisfied by a selected product to launch a particular tool.	varchar	256
PROP1_VALUE	First condition value to be satisfied by a selected product to launch a particular tool.	varchar	256
PROP2_KEY	Second condition name to be satisfied by a selected product to launch a particular tool.	varchar	256
PROP2_VALUE	Second condition value to be satisfied by a selected product to launch a particular tool.	varchar	256
TOOL_ID	The tool to be used for launching the application.	int	
PARAMETERS	Link to that application.	varchar	256
IP_SELECTED	Selected IP Address option.	smallint	
WWN_SELECTED	Selected WWN option.	smallint	

Zoning 1

TABLE 212 ZONE_DB

Field	Definition	Format	Size
ID*	PK of the owning fabric.	int	
FABRIC_ID	Zone DB name for offline Zone DBs.	int	
NAME	Offline Zone DB (1 = offline).	varchar	256
OFFLINE	Created timestamp.	smallint	
CREATED	Last modified timestamp.	timestamp	
LAST_MODIFIED	Last modified timestamp.	timestamp	
LAST_APPLIED	Last saved to switch timestamp.	timestamp	
CREATED_BY	Created by user name.	varchar	128
LAST_MODIFIED_BY	Last modified by user name.	varchar	128
LAST_APPLIED_BY	Last saved to switch user name.	varchar	128
DEFAULT_ZONE_STATUS	All access or no access when no active zone configuration.	smallint	
ZONE_TXN_SUPPORTED	Zoning commands support transaction.	smallint	

TABLE 212 ZONE_DB (Continued)

Field	Definition	Format	Size
MCDATA_DEFAULT_ZONE	McData switch default zoning mode.	smallint	
MCDATA_SAFE_ZONE	McData switch safe zoning mode.	smallint	
ZONE_CONFIG_SIZE	Zone configuration string length.	int	

TABLE 213 ZONE_DB_USERS

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK of the owning zone DB.	int	
USER_NAME	List of users currently editing this zone DB.	varchar	128

TABLE 214 LSAN_ZONE

Field	Definition	Format	Size
ID*		int	
BB_FABRIC_ID	Backbone fabric DB ID.	int	
EDGE_FABRIC_ID	FID assigned to edge fabric.	int	
NAME	LSAN zone name.	varchar	128

TABLE 215 LSAN_ZONE_MEMBER

Field	Definition	Format	Size
LSAN_ZONE_ID*	LSAN_ZONE record reference.	int	
MEMBER_PORT_WWN*	Zone member WWN.	char	23

TABLE 216 ZONE_DB_CONTENT

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK of the owning offline zone DB.	int	
CONTENT	Saved online content before offline was saved to switch.	long varchar	
TI_CONTENT	TI_CONTENT saved online TI zone content before offline was saved to switch.	long varchar	
DEFINED		long varchar	
ACTIVE		long varchar	

Zoning 2

TABLE 217 ZONE_ALIAS_IN_ZONE

Field	Definition	Format	Size
ZONE_ALIAS_ID*	PK of the zone alias.	int	
ZONE_ID*	PK of the zone.	int	23

TABLE 218 ZONE_ALIAS

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK of the owning ZONE_DB.	int	
NAME	The zone alias name.	varchar	64

TABLE 219 ZONE_ALIAS_MEMBER

Field	Definition	Format	Size
ID*		int	
TYPE	Zone alias member type: 2 = WWN 4 = D,P	smallint	
VALUE	Member value (D,P or WWN).	varchar	256
ZONE_ALIAS_ID	PK of the owning zone alias.	int	

TABLE 220 ZONE_IN-ZONE_SET

Field	Definition	Format	Size
ZONE_SET_ID*	PK of the owning zone set.	INT	
ZONE_ID*	PK of the owning zone.	INT	

TABLE 221 ZONE

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK the owning ZONE_DB.	int	
NAME	The zone name.	varchar	64
TYPE	The zone type.	int	
SUB_TYPE	The zone subtype.	int	
ACTIVATE	For TI zones only, zone is activated.	smallint	
FAILOVER_ENABLED	For TI zones only, failover is enabled.	smallint	

TABLE 222 ZONE_DB

Field	Definition	Format	Size
ID*		int	
FABRIC_ID	PK of the owning fabric.		
NAME	Zone DB name for offline Zone DBs.	varchar	256
OFFLINE	Offline Zone DB (1 = offline).	smallint	
CREATED	Created timestamp.	timestamp	
LAST_MODIFIED	Last modified timestamp.	timestamp	
LAST_APPLIED	Last saved to switch timestamp.	timestamp	
CREATED_BY	Created by user name.	varchar	128
LAST_MODIFIED_BY	Last modified by user name.	varchar	128
LAST_APPLIED_BY	Last saved to switch user name.	varchar	128
DEFAULT_ZONE_STATUS	All access or no access when no active zone configuration.	smallint	
ZONE_TXN_SUPPORTED	Zoning commands support transaction.	smallint	
MCDATA_DEFAULT_ZONE	McData switch default zoning mode.	smallint	
MCDATA_SAFE_ZONE	McData switch safe zoning mode.	smallint	
ZONE_CONFIG_SIZE	Zone configuration string length.	int	

TABLE 223 ZONE_SET

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK of owning zone DB.	int	
NAME	Zone set name.	varchar	64
ACTIVE	1 = active zone configuration; otherwise, 0.	smallint	

TABLE 224 ZONE_MEMBER

Field	Definition	Format	Size
ID*		int	
TYPE	Member type: 2 = WWN 4 = D,P	smallint	
VALUE	Member value (D,P or WWN).	varchar	256
ZONE_ID	PK of owning zone.	int	

Index

A

accessing
    FTP server folder, *98*
ACK emulation, device level, *252*
activating
    event policies, *187*
    zone configuration, *391*
active sessions, viewing, *63*
adding, *180*
    destination for syslog forwarding, *205*
    event policies, *180*
    ISL offline policies, *181*
    PM threshold crossed policies, *182*
    property labels, *136*
    security violation policies, *183*
    traffic isolation zone members, *399*
    V1 destination, SNMP traps, *200*
    V3 destination, SNMP traps, *201*
    zone members, *381*
    zones, *391*
advanced filtering
    setting up, *197*
alerts, zone configuration comparison, *404*
asset polling, configuring, *107*
associating HBAs to servers, *144*

B

backup
    changing interval, *76*
    configuring to hard drive, *72*
    configuring to network drive, *73*
    configuring to writable CD, *71*
    data, *70*
    disabling, *75*
    enabling, *75*
    immediate, *76*
    management server, *70*
    reviewing events, *77*
    starting, *76*
    status, determining, *15*
    viewing status, *75*
broadcast messages
    defining, *184*

C

call home
    status, determining, *15*
certificates
    importing using the CLI, *431*, *438*
    storing the public key, *339*
changing
    database passwords, *63*
    passwords, *62*
    port display, *119*
    port label, *118*
    product label, *118*
    view options, *65*
CHAP secret
    setting, *94*
clearing fabric zone database, *407*
clearing port counters, performance, *218*
client export port, configuring, *96*
client/server
    firewall requirements, *58*
collapsing groups, *119*
color, changing, *117*, *118*
community strings
    reverting to default, *43*
comparing
    zone databases, *402*
compression
    enabling, *249*
concepts, FCIP, *234*
configuration
    storage encryption privileges, *315*
configuration files, saving, *132*
configuration repository management, overview, *131*

Configure menu, *5*
configuring
asset polling, *107*
client export port, *96*
discovery, *39*, *97*
e-mail notification, *196*
encrypted storage in a multi-path environment, *355*
explicit server IP address, *103*
external FTP server, *100*
FCIP advanced settings, *249*
FCIP tunnels, *245*
FICON emulation, *252*
FTP server, *98*
internal FTP server, *99*
IP configuration, *102*
IP interfaces, *245*
IP routes, *245*
IPSec and IKE policies, *251*
login banner, *95*
login security, *94*
memory allocation, *106*
security authentication using the GUI, *230*
server name, *93*
server port, *108*
smart cards, *316*
SNMP credentials, *42*
software, *96*
support mode settings, *109*
traffic isolation zoning, *397*
zoning for the SAN, *379*
configuring zoning, *379*
connected ports, showing, *156*
connections
status, determining, *15*
connections between a switch and an LKM key vault, *330*
connections, changing display of, *116*
content
broadcast messages, *184*
copying
log entries, *173*
log entry parts, *173*
master log, *176*
master log parts, *176*
zones, *407*
creating
traffic isolation zone, *398*
zone, *380*
zone alias, *387*
zone configuration, *389*
zone members by alias, *384*
zone members by domain,port, *383*
zone members by WWN, *382*
zone sets, *389*
cryptocfg command
--export, *430*, *436*
--import, *429*, *431*, *436*, *438*
--reg -keyvault, *440*, *442*
--set -keyvault, *443*
--show -groupcfg, *433*

D

data
real time performance, *215*
data backup, *70*
data restore, *77*
database fields
Sybase and Derby, *455*
database, restoring, *127*
deactivating
event policies, *187*
deactivating zone configuration, *393*
default background color, changing, *118*
default community strings, *43*
default desktop color, changing, *118*
default zone (fabrics)
disabling, *385*
enabling, *385*
defining
broadcast messages, *184*
e-mail messages, *186*, *187*
launch script path, *185*
DEK (data encryption keys), *427*
deleting
event policies, *188*
fabrics, *43*
FCIP tunnels, *260*
property labels, *137*
reports, *222*
technical support information, *166*
zone alias, *406*
zone configuration, *406*
zones, *405*

deleting firmware files from
firmware repository, *140*
deleting servers, *144*
Derby database fields, *455*
destination
adding for syslog forwarding, *205*
editing for SNMP traps, *202*
editing for syslog forwarding, *206*
removing for SNMP traps, *202*
removing for syslog forwarding, *206*
device
adding names, *89*
removing name, *90*
device icons, *16*
device properties, *133*
viewing, *133*
device properties dialog boxes, customizing, *133*
device tips
configuring, *83*
device tips, turning on and off, *86*
device tips, viewing, *86*
diagnostics
types of tests, *229*
directory structure overview, backing up, *71*
disabling
default zone for fabrics, *385*
FCIP tunnels, *259, 260*
login banner, *95*
port connectivity view filter, *152*
ports, *150*
safe zoning mode, *386*
syslog forwarding, *207*
traffic isolation zone, *400*
traffic isolation zone failover, *401*
disabling backup, *75*
disabling SNMP informs, *203*
disabling trap forwarding, *202*
Discover menu, *5*
discovering a fabric, *37*
discovery, *37*
configuring, *39, 97*
description of, *228*
in-band, enabling, *39*
out-of-band, enabling, *39*
setting up, *39*
SNMP version, *39*
state, *50*
troubleshooting, *51*
display
end nodes, *80*
display, FICON, *79*
displaying
event details, *174, 175*
FCIP performance graphs for Ethernet ports, *261*
FCIP performance graphs for FC ports, *261*
firmware repository, *138*
link details for FCIP tunnels, *261*
master log event details, *174, 175*
downloading
firmware, *141*
duplicate names,fixing, *88*
duplicating
event policies, *188*
ISL offline policies, *189*
PM threshold crossed policies, *190*
security violation policies, *191*
zone alias, *408*
zone configuration, *408*
zones, *407*

E

Edit menu, *3*
editing
destination for syslog forwarding, *206*
destination, SNMP traps, *202*
event policies, *192*
ISL offline policies, *193*
PM threshold crossed policies, *194*
property fields, *137*
property labels, *136*
security violation policies, *195*
zone alias, *387*
Element Manager, launching
launching Element Manager, *112*
e-mail filter override, *227*
e-mail messages
defining, *186, 187*
e-mail notification
configuring, *196*
emailing
technical support information, *166*
enable SSL, *108*

enabling
compression, fast write, tape pipelining, *249*
default zone for fabrics, *385*
FCIP tunnels, *259, 260*
port connectivity view filter, *152*
ports, *150*
safe zoning mode, *386*
syslog forwarding, *206*
traffic isolation zone, *400*
traffic isolation zone failover, *401*
enabling backup, *75*
enabling SNMP informs, *203*
enabling trap forwarding, *200*
encryption
adding a target, *334*
adding new LUNs, *335*
configuration planning for the management application, *314*
configure dialog box, *316*
configuring hosts to access encryption targets, *335*
configuring in a multi-path environment, *355*
gathering information before using the setup wizard, *314*
launching the encryption target properties dialog box, *335*
launching the encryption targets dialog box, *333*
moving a target to a different encryption engine, *334*
removing a target, *334*
selecting mode for LUNs, *362*
viewing and editing group properties, *324*
encryption engines
adding to HA clusters, *329*
effects of zeroizing, *373*
recovering from zeroizing, *373*
removing from HA clusters, *329*
support for tape pools, *331*
zeroizing, *373*
encryption group
adding a switch using the management application, *344*
confirming configuration status, *341*
creating using the encryption setup wizard, *336*
selecting the key vault type, *338*
encryption group properties
using the restore master key, *373*
viewing encryption group properties, *324*
encryption group properties dialog box
General tab, *325*
HA Clusters tab, *329, 348*
Link Keys tab, *329, 330*
Members tab, *325*
Tape Pools tab, *331*
encryption properties
viewing properties, *320*
encryption switch or group, removing using the management application, *326*
encryption targets
adding to virtual targets and virtual initiators within the encryption switch, *350*
configuring hosts for, *357*
using the dialog box, *333*
using the dialog box to add Disk LUNs, *358*
end nodes
display, *80*
Ethernet events
disabling, *82*
enabling, *81*
event details
displaying, *174, 175*
event filtering, advanced, *197*
event logs, *172*
copying entries, *173*
copying parts, *173*
exporting entries, *174*
viewing, *172*
event management
overview, *171*
event notification
configuring e-mail notification, *196*
event notification, description, *196*
event policies, *180*
activating, *187*
broadcast message, *184*
deactivating, *187*
deleting, *188*
description, *179*
duplicating, *188*
editing, *192*
e-mail messages, *186, 187*
ISL offline policy, *181*
ISL offline, duplicating, *189*
ISL offline, editing, *193*
launch scripts, *185*

PM threshold crossed policy, *182*
PM threshold crossed, duplicating, *190*
PM threshold crossed, editing, *194*
security violation policy, *183*
security violation, duplicating, *191*
security violation, editing, *195*
viewing events, *195*
event types, *179, 227*
events
Ethernet, *81*
event types, *179, 227*
filtering, *177, 227*
monitoring methods, *171*
policy actions, *180*
policy types, *179*
storage, *82*
viewing, *195*
expanding groups, *119*
explicit server IP address
configuring, *103*
export commands
–export, *430, 436*
exporting
log entries, *174*
master log, *177*
real time performance data, *218*
reports, *221*
zone alias, *389*
external FTP server
configuring, *100*

F

Fabric OS
seed switch version, *53*
Fabric OS feature listing, *31*
fabrics
deleting, *43*
discovering, *37*
IPv6 discovery, *38*
monitoring, *51*
status, determining, *15*
zone database, clearing, *407*
fast write, enabling, *249*
Fastwrite, *240*
FC Address
for inactive iSCSI devices, *153, 159*
FC routing module, *113*
FCIP
advanced settings
configuring, *249*
connection properties
viewing, *253*
Ethernet connection
troubleshooting, *266*
Ethernet port properties
viewing, *256*
fast write, *243*
Fastwrite, *240*
FC port properties
viewing, *255*
IP compression, *239*
IPsec implementation, *239*
performance graphs, Ethernet ports
displaying, *261*
performance graphs, FC ports
displaying, *261*
properties
viewing, *254*
services
licensing, *234*
Tape Pipelining, *240*
tape pipelining, *243*
tunneling, *234*
tunnels
configuring, *245*
deleting, *260*
disabling, *259, 260*
displaying link details, *261*
enabling, *259, 260*
modifying, *257*
FCIP configuration
advanced settings, *243, 249*
fast write and tape pipelining, *243*
IP interfaces, *245*
IP routes, *245*
FCIP configuration, guidelines, *242*
FCR configuration, launching, *113*
feature
licensing requirements, *31*
feature-to-firmware requirements, *31*
Fibre Channel over IP, *234*
FICON
configuring emulation, *252*
display
resetting, *79*
setting, *79*

filtering
events for users, *227*
master log events, *177*
port connectivity view results, *151*
real time performance data, *217*
firmware
deleting files from repository, *140*
downloading, *141*
management, overview, *138*
overwriting, *141*
firmware repository
deleting firmware files, *140*
displaying, *138*
importing into, *139*
flyovers
configuring, *83*
turning on and off, *86*
viewing, *86*
FTP
overview, *98*
server
accessing the folder, *98*
configuring, *98*
testing, *101*

G

generating
performance graph, *216*
reports, *220*
zoning reports, *222*
graphs
FCIP performance for Ethernet ports, *261*
FCIP performance for FC ports, *261*
group background color, changing, *117*
grouping
overview, *119*
groups
collapsing, *119*
expanding, *119*
overview, *119*
groups, changing color, *117*
groups, icons, *17*
guidelines
FCIP configuration, *242*
advanced settings, *243*

H

HA clusters
creating, *347*
removing engines from, *348*
requirements for, *347*
swapping engines in, *349*
HBAs
associating to servers, *144*
unassociating, *146*
HCM
features, *228*
software overview, *228*
statistics monitoring, *229*
HCM Agent, launching, *114*, *229*
Help menu, *9*
host management, remote, *228*
host server
registering as trap recipient, *199*
registering for syslog forwarding, *205*
removing as trap recipient, *200*
removing for syslog forwarding, *205*
HP SKM, *440*
http
//www.gemalto.com/readers/index.html, *316*

I

icons
device, *16*
products, *16*
IKE, *243*
IKE policies
configuring, *251*
immediate technical support information collection, *165*
import commands, --import, *429*, *431*, *436*, *438*
importing
firmware files and release notes, *139*
inactive iSCSI devices, identifying, *153*, *159*
in-band discovery, enabling, *39*
internal FTP server
configuring, *99*
IP configuration, *102*
IP frames, *234*
IP interfaces, configuring, *245*
IP routes, configuring, *245*
IPSec
limitations, *243*

IPsec
FCIP, *239*
IPSec policies, *243*
configuring, *251*
iSCSI devices, identifying inactive, *153*, *159*
ISL offline policies
adding, *181*
duplicating, *189*
editing, *193*

K

key vaults
adding or changing using the management application, *339*
connection from switch, *330*
entering the IP address or host name for, *338*
entering the name of the file holding the certificate, *338*
setting up RKM, *440*

L

launch script path
defining, *185*
launch scripts, *185*
requirements, *185*
launching
Server Management Console, *123*
launching FCR configuration, *113*
launching HCM Agent, *114*, *229*
launching Telnet, *112*
launching Web Tools, *113*
layout, changing, *116*
layout, overview, *115*
licensing
FCIP services, *234*
Lifetime Key Manager (LKM)
description of, *428*
link details
displaying for FCIP tunnels, *261*
link keys, creating, *330*
listing
zone members, *411*
LKM
creating link keys, *330*
support for high availability (HA), *434*, *447*
log entries
copying, *173*
copying parts, *173*
exporting, *174*
logging in
remote client, *61*
server, *60*
login banner
configuring, *95*
disabling, *95*
login security
configuring, *94*
logon conflicts, *391*
logs
event, *172*
LUN
choosing to be added to an encryption target container, *361*
editing a re-keying interval, *360*
selecting the encryption mode, *360*

M

Main window
master log, *13*
menu bar, *3*
minimap, *14*
Management application
server and client, *58*
management application
main window, *2*
user interface, *1*
Management application feature listing, *31*
Management application services
monitoring and managing, *124*
management server
registering as trap recipient, *199*
registering for syslog forwarding, *204*
management software components, *228*
managing
zone configuration comparison alerts, *404*

master key
active, *363*
alternate, *364*
backup, *364*
create new master key, *364*
creating a new, *372*
description of, *363*
reasons they are disabled, *364*
restore master key, *364*
saving to a file, *364*
master log, *13*
copying, *176*
copying parts, *176*
displaying, *174, 175*
exporting, *177*
filtering events, *177*
McDATA fabric mode, *386*
memory allocation
configuration, *106*
configuring asset polling, *107*
menu bar, *3*
Configure, *5*
Discover, *5*
Edit, *3*
Help, *9*
Monitor, *7*
SAN, *3*
Tools, *9*
View, *3*
M-EOS feature listing, *31*
merging
zone databases, *394*
minimap, *14*
anchoring, *14*
attaching, *14*
detaching, *14*
floating, *14*
resizing, *14*
modifying
FCIP tunnels, *257*
Monitor menu, *7*
monitoring fabrics, *51*
monitoring statistics, *229*
multi-path configuration for encrypted storage using the Management application, *355*

N

names
adding to existing device, *89*
adding to new device, *90*
editing, *90*
exporting, *91*
fixing duplicates, *88*
importing, *91*
removing from device, *90*
searching by, *92*
setting as non-unique, *88*
setting as unique, *87*
viewing, *89*
names, overview, *87*
naming conventions, *378*
NetApp Lifetime Key Manager (LKM), description of, *428*
NetApp LKM key vaults
effects of zeroizing, *373*
new device, adding name, *90*

O

offline ports, display, *159*
out-of-band discovery
setting up, *39*
overwriting
firmware, *141*

P

passwords
changing, *62*
database, changing, *63*
performance
clearing port counters, *218*
performance data
real time, *215*
performance graph
generating, *216*
performance monitoring
overview, *209*
performance measures, *209*

physical map
default background color, changing, *118*
displaying connections, *116*
group background color, changing, *117*
layout, changing, *116*
layout, overview, *115*
levels of detail, *66*
port display, changing, *119*
port label, changing, *118*
product label, changing, *118*
showing connected ports, *156*
viewing port types, *156*
viewing ports, *153*
zooming in, *65*
zooming out, *65*
PM threshold crossed policies
adding, *182*
duplicating, *190*
editing, *194*
policies
IKE, *243*
IPSec, *243*
policy actions, *180*
policy triggers, *180*
policy types, *179*
port connection properties, viewing, *157*
port connectivity view
disabling filter, *152*
enabling filter, *152*
filtering results, *151*
refreshing, *150*
resetting filter, *152*
viewing details, *152*
port connectivity, viewing, *147*
port display, changing, *119*
port label, changing, *118*
port optics
refreshing, *160*
viewing, *159*
port properties, *153*
port status, determining, *159*
port types, viewing, *156*
ports, *147*
determining status, *159*
disabling, *150*
enabling, *150*
showing connected, *156*
view connectivity, *147*
viewing, *153*
viewing connection properties, *157*
viewing types, *156*
primary FCS, *37*
printing
reports, *221*
privileges, user, *315*
product label, changing, *118*
Product list, *11*
columns, *11*
products
icons, *16*
status, determining, *15*
properties
FCIP connection, *253*
FCIP Ethernet port, *256*
FCIP FC port, *255*
general FCIP, *254*
property fields
editing, *137*
property labels
adding, *136*
deleting, *137*
editing, *136*

R

real time performance, *215*
exporting data, *218*
filtering data, *217*
graph, *216*
refreshing
port optics view, *160*
zone databases, *394*
refreshing the port connectivity view, *150*
register commands
--reg -keyvault, *440*, *442*
registering
host server, *199*
host server for syslog forwarding, *205*
management server, *199*
management server for syslog forwarding, *204*
registration
SNMP traps, *199*
remote client
logging in, *61*
remote host management, *228*

removing
destination for syslog forwarding, *206*
destination, SNMP traps, *202*
host server, *200*
host server for syslog forwarding, *205*
members from zone, *411*
objects from zone alias, *388*
servers, *144*
zone from zone configuration, *412*
zones from zone configuration, *412*
renaming
zone alias, *389*
zone configuration, *413*
zones, *412*
renaming servers, *143*
replacing
zone members, *414*
report types, *219*
reports
deleting, *222*
exporting, *221*
generating, *220*
printing, *221*
viewing, *220*
zoning, *222*
requirements
launch scripts, *185*
resetting
port connectivity view filter, *152*
restore data, *77*
restore master key wizard, *373*
restoring
database, *127*
reviewing
backup events, *77*
RKM key vaults
setting up, *440*
RSA Key Manager (RKM)
description of, *436*, *440*, *451*

S

safe zoning mode
disabling, *386*
enabling, *386*
SAN
zoning, *379*
SAN menu, *3*
saving
switch configuration files, *132*
zone databases to switch, *396*
scheduling
technical support information collection, *164*
search
names, *92*
WWN, *92*
searching
members in zones, *409*
Potential Members list, *409*
zones in zone configuration, *410*
Zones list, *410*
security
configuring, *93*
security authentication
configuring using the GUI, *230*
security tab on management application
using to back up a master key, *328*
using to create a master key, *328*
using to restore a master key, *328*
security violation policies
adding, *183*
duplicating, *191*
editing, *195*
seed switch, *37*, *53*
change requirements, *53*
changing, *54*
FCS policy, *38*
sequential devices, *240*, *244*
server IP address, explicit, *103*
Server Management Console
about, *123*
launching, *123*
server name
configuring, *93*
server name, determining, *15*
server port
configuring, *108*
enable SSL, *108*
server port numbers, changing, *126*
server properties, viewing, *64*
servers
associating to HBAs, *144*
determining name, *15*
logging in, *60*
removing, *144*
renaming, *143*
set commands
--set -keyvault, *443*

setting
CHAP secret, *94*
setting up
advanced filtering, *197*
discovery, *39*
show commands --show -groupcfg, *433*
showing levels of detail, physical map, *66*
showing ports
connected, *156*
procedure, *153*
SKM, *440*
smart cards
configuring, *316*
removing using the management application, *375*
saving to a file, *375*
tracking using the management application, *375*
SNMP credentials, configuring, *42*
SNMP informs, disabling, *203*
SNMP informs, enabling, *203*
SNMP traps
adding V1 destination, *200*
adding V3 destination, *201*
editing a destination, *202*
registering a different host server, *199*
registering the management server, *199*
removing a destination, *202*
removing the host server, *200*
trap forwarding, disabling, *202*
trap forwarding, enabling, *200*
SNMP traps, registration and forwarding, *199*
software configuration, *96*
start monitoring, *52*
status
backup, *75*
discovery, *50*
status bar, *15*
stop monitoring, *52*
storage encryption
configuration privileges, *315*
configuring, *351*
confirming the configuration status, *355*
selecting the encryption engine for configuration, *352*
selecting the hosts, *353*
specifying a name for the target container, *353*
storage encryption security
privileges for, *315*
storage events
configuring, *82*
support mode
configuring, *109*
switch encryption configuration
confirm configuration using the management application, *345*
designate switch membership using the management application, *344*
specify public key certificate filename using the management application, *345*
switch removal, consequences of, *326*
Sybase database fields, *455*
syslog forwarding
adding a destination, *205*
description, *204*, *228*
disabling, *207*
editing a destination, *206*
enabling, *206*
registering host server, *205*
registering management server, *204*
removing a destination, *206*
removing host server, *205*

T

tab
Services (SMC), *127*
tab Ports (SMC), *126*
tab Technical Support Information (SMC), *128*
tab, Services (SMC), *124*
tables
capability database fields, *456–457*
client_view database fields, *457–459*
collector database fields, *460–463*
config database fields, *463–465*
connected end devices database fields, *465*
device database fields, *466–473*
EE-monitor database fields, *473–475*
encryption container database fields, *??–497*
encryption device database fields, *??–497*
event/FM database fields, *475–481*
fabric database fields, *481–483*
FC port status database fields, *484–486*
FCIP database fields, *487–490*
FCIP tunnel stats database fields, *490–492*
GigE port stats database fields, *492–494*
ISL database fields, *494–497*
license database fields, *497*
Meta SAN database fields, *498–500*
network database fields, *500–501*
others database fields, *501*
port fencing database fields, *502*

quartz database fields, *503–505*
reports database fields, *506*
role based access control database fields, *506–508*
SNMP database fields, *509–511*
stats database fields, *512–??*
switch database fields, *514–518*
switch details database fields, *519–523*
switch port database fields, *524–529*
switch SNMP info database fields, *529–530*
threshold database fields, *531–532*
UI database fields, *532–533*
zoning 1 database fields, *533–534*
zoning 2 database fields, *535–536*
Tape Pipelining, *240*
tape pipelining, *244*
enabling, *249*
tape pools
adding, *332*
description of, *331*
identifying using a name or a number, *332*
modifying, *331*
removing, *331*
tape read and write acceleration, *240*
tape write acceleration, *244*
technical support information
deleting, *166*
emailing, *166*
immediate, *165*
technical support information collection
scheduling, *164*
technical support information, capturing, *128*
technical support information, viewing, *165*
Telnet
launching session, *112*
testing
FTP server, *101*
third-party tools
starting, *111*
TIN/TUP emulation, *252*
tips, turning on and off, *86*
tips, viewing, *86*
tool tips, turning on and off, *86*
tool tips, viewing, *86*
toolbox, *13*
Tools menu, *9*
tooltips
configuring, *83*
topolgy
viewing ports, *153*
topology
changing port display, *119*
changing port label, *118*
changing product label, *118*
displaying connections, *116*
group background color, changing, *117*
showing connected ports, *156*
viewing port types, *156*
topology, changing layout, *116*
topology, overview, *115*
topology, See also physical map
total user count, *15*
traffic isolation zone
adding members, *399*
creating, *398*
disabling, *400*
disabling failover, *401*
enabling, *400*
enabling failover, *401*
traffic isolation zoning, *397*
configuring, *397*
trap forwarding
disabling, *202*
enabling, *200*
triggers, *180*
troubleshooting
discovery, *51*
FCIP Ethernet connections, *266*
tunnels, configuring, *245*

U

unassociating, HBA to server, *146*
user ID, determining, *15*
user interface, description, *1*
user privileges
defined, *315*
resource groups, *315*
users
disconnecting, *64*
filtering events for, *227*
users, total, *15*
using from encryption group properties dialog, *373*

V

V1 destination
adding, *200*
V3 destination
adding, *201*
VE_Ports, *241*
view all tab, *11*
View menu, *3*
view options, changing, *65*
View window
product list, *11*
view all tab, *11*
View window, toolbox, *13*
viewing
device properties, *133*
disabling port connectivity filter, *152*
enabling port connectivity filter, *152*
event logs, *172*
events, *195*
FCIP connection properties, *253*
FCIP Ethernet port properties, *256*
FCIP FC port properties, *255*
filtering port connectivity, *151*
general FCIP properties, *254*
offline ports, *159*
port connectivity, *147*
port connectivity details, *152*
port optics, *159*
port properties, *153*
port types, *156*
ports, *153*
reports, *220*
restting port connectivity filter, *152*
technical support information, *165*
zooming in, *65*
zooming out, *65*
viewing ports
connection properties, *157*

W

Web Tools, launching, *113*
WWN
searching by, *92*

Z

zeroizing
effects of using on encryption engine, *373*
zone
adding to comnfiguration, *391*
alias, *387*
creating, *380*
removing, *412*
traffic isolation, adding members, *399*
traffic isolation, creating, *398*
traffic isolation, disabling, *400*
traffic isolation, disabling failover, *401*
traffic isolation, enabling, *400*
traffic isolation, enabling failover, *401*
zone alias
creating, *387*
deleting, *406*
editing, *387*
exporting, *389*
zone alias, duplicating, *408*
zone alias, removing objects, *388*
zone alias, renaming, *389*
zone configuration
activating, *391*
adding zones, *391*
creating, *389*
deactivating, *393*
deleting, *406*
duplicating, *408*
finding member in Zones list, *410*
removing a zone, *412*
removing zones, *412*
renaming, *413*
zone configuration comparison alerts
managing, *404*
zone configuration member
finding in Zones list, *410*
zone databases
comparing, *402*
merging, *394*
refreshing, *394*
saving to switch, *396*

zone members
adding to zone, *381*
creating in zone by alias, *384*
creating in zone by domain,port, *383*
creating in zone by WWN, *382*
finding in Potential Members list, *409*
finding in zones, *409*
listing, *411*
removing from zone, *411*
replacing, *414*
zone set
creating, *389*
naming conventions, *378*
zone set. See zone configuration
zones
deleting, *405*
duplicating, *407*
finding in zone configuration, *410*
removing from zone configuration, *412*
renaming, *412*
zoning
accessing, *378*
configuration overview, *379*
configuring for the SAN, *379*
invalid names, *379*
naming conventions, *378, 379*
online, *378*
overview, *377*
traffic isolation, *397*
traffic isolation, configuring, *397*
zoning administration, *402*
zoning configuration
overview, *379*
zoning reports
generating, *222*
zooming in, *65*
zooming out, *65*